The Open University

M303

Further pure mathematics

Book B

Groups

This publication forms part of the Open University module M303 *Further pure mathematics*. Details of this and other Open University modules can be obtained from Student Recruitment, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)300 303 5303; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2014. Second edition 2016.

Copyright © 2014, 2016 The Open University

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS (website www.cla.co.uk).

Open University materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or retransmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed in the United Kingdom by Halstan & Co. Ltd, Amersham, Bucks.

ISBN 978 1 4730 2037 5

2.1

Contents

Chapter 5 Examples of groups **1**

Introduction **3**

1 Axioms and examples **4**
1.1 Group axioms 4
1.2 Permutations 10
1.3 Symmetries of figures 11
1.4 Cyclic groups 14
1.5 Groups from modular arithmetic 15

2 Subgroups and cosets **16**
2.1 Subgroups 17
2.2 Cosets and Lagrange's Theorem 21

3 Normal subgroups and quotient groups **26**
3.1 Normal subgroups 26
3.2 Quotient groups 33

4 Isomorphisms and homomorphisms **37**
4.1 Isomorphisms 37
4.2 Homomorphisms 45
4.3 The Correspondence Theorem 51

5 The group of permutations on four elements **55**

Learning outcomes **61**

Solutions to exercises **62**

Chapter 6 Towards classification **85**

Introduction **87**

1 Direct products **88**
1.1 The external direct product of two groups 88
1.2 Internal direct products 91

2 Cyclic groups **101**
2.1 The classification of cyclic groups 102
2.2 Subgroups and quotient groups of cyclic groups 103
2.3 Direct products of cyclic groups 107

3 Group actions **115**
3.1 Actions, orbits and stabilisers 115
3.2 Cayley's Theorem 126
3.3 Cauchy's Theorem 129
3.4 Finite abelian groups 131

Learning outcomes **135**

Solutions to exercises **136**

Chapter 7 Finite groups **149**

Introduction **151**

1 Describing groups **151**
1.1 Generators and relations 152
1.2 Dicyclic groups 158
1.3 Describing subgroups using generators 161

2 Conjugates, centralisers and centres **165**
2.1 Conjugates 165
2.2 Conjugacy classes 166
2.3 Centralisers 169
2.4 Centres 170
2.5 Conjugates and centralisers 172
2.6 Groups of order p^2 174

3 Groups of small order **175**
3.1 Groups of order p 175
3.2 Groups of order p^2 revisited 175
3.3 Groups of order $2p$ 176
3.4 Groups of order 8 178
3.5 Groups of order 12 180

4 Finite p-groups **185**
4.1 p-groups and their subgroups 185
4.2 Soluble groups 189

Learning outcomes **192**

Solutions to exercises **193**

Chapter 8 The Sylow Theorems **203**

Introduction **205**

1 The Sylow Theorems **206**
1.1 Sylow p-subgroups 206
1.2 Sylow's First and Second Theorems 215
1.3 Sylow's Third Theorem 222

2 Applications of the Sylow Theorems **224**
2.1 Finite abelian groups 224
2.2 Exercises using the Sylow Theorems 226

3 Subgroups of prime power order **231**

4 Groups of order $2p^2$ **235**

Learning outcomes **237**

Solutions to exercises **238**

Index **257**

Chapter 5

Examples of groups

Introduction

In this book we discuss groups. Much of the early material should be familiar from your previous studies. The main aim of the book is to introduce results that can be used to describe the structure of finite groups.

In mathematics, a description of an infinite class of mathematical objects often comes in the form of a *classification*, that is, a list where the objects in question are grouped into finitely many categories according to some structural characteristics. Thus, the most general problem that we could pose for finite groups asks for a classification of them. Unfortunately, this problem seems hopelessly hard, but less general classification results can be obtained by imposing some additional conditions on the finite groups under consideration.

It is the importance of finite groups in applications, as well as in other branches of mathematics, that motivated the interest in a classification: finite groups provide sophisticated tools for the study and analysis of patterns of all sorts, for example the patterns found in the solutions to polynomial equations, the patterns found in the symmetries of crystals, and more recently certain patterns found in viruses.

A finite group G is said to be *simple* if its only normal subgroups are the identity subgroup and G itself. This means, in some sense, that a group is simple if it cannot be decomposed into two smaller groups. Simple groups are very important in classification: there is a theorem, proved by Jordan (1838–1922) and Hölder (1859–1937) towards the end of the nineteenth century, that tells us that finite simple groups are the building blocks of finite groups, rather like prime numbers are the building blocks of the integers. This is why much of the work on finite groups in the latter half of the twentieth century was about trying to identify all finite *simple* groups.

The classification of finite simple groups was finally achieved around 2004, after a joint effort that stretched over 50 years and involved many mathematicians, but the details are well beyond the scope of this module. However, by the end of the book you should be familiar with several classes of groups and be able to determine the possible structures for groups of some given orders.

This chapter introduces some basic features of groups. In Section 1 you are reminded of the group axioms, and of groups arising from symmetries of plane figures and from modular arithmetic. You will review subgroups and cosets in Section 2, and normal subgroups and quotient groups in Section 3. Section 4 covers group isomorphisms and homomorphisms. Lagrange's Theorem, the First Isomorphism Theorem and the Correspondence Theorem are stated and proved in Sections 2 and 4. In the final section you will work in some detail with the group of permutations on four elements. The exercises in this section provide a concrete illustration of the ideas of the whole chapter.

Chapter guide

In this chapter, we assume you have some familiarity with groups and their basic properties from your previous studies. One of the aims is to introduce you to many examples of both finite and infinite groups that will recur later in Book B. Some of these examples help to highlight the fact that groups can have several different but equivalent representations. This is the longest chapter in Book B, but a lot of the material will be revision.

The first three sections are of roughly equal length and should mostly be revision. The last part of Section 4 proves the Correspondence Theorem, an important result you should make sure you are familiar with. Section 5 consists mostly of exercises designed to apply the notions of the first four sections to a specific finite group.

1 Axioms and examples

This section reminds you of the axioms for a group and looks at some examples that will prepare you for the rest of the chapter. Some of the examples may be familiar to you, some may not be. Since this topic demands real familiarity with many of these examples, we ask you to work carefully through all the exercises.

1.1 Group axioms

You may remember from your previous studies that the group axioms are an abstraction of certain properties shared by various sets of numbers, functions, transformations, etc., equipped with an operation to combine the elements of the set. The abstraction process leads to the following definition.

Definition 1.1 *Group axioms*

A set G together with a binary operation $\circ$ defined on G is a **group** if the following axioms are satisfied.

G1 Closure For all pairs x, y of elements in G, $x \circ y$ is also in G.

G2 Identity There is an **identity element** – e, say – in G with the property that, for any element x in G,

$$e \circ x = x = x \circ e.$$

G3 Inverses For each element x in G, there is an **inverse element** x^{-1} in G with the property that

$$x \circ x^{-1} = e = x^{-1} \circ x,$$

where e is the identity element of G.

G4 Associativity For all choices of elements x, y, z in G, we have

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Although the closure axiom follows from the definition of a binary operation, we include it for clarity.

The set G is sometimes called the **underlying set** of the group, and we should really say that $(G, \circ)$, rather than G, is a group if the axioms are satisfied; that is, we should always make explicit reference to the set *and* the operation when talking about groups. However, to avoid clumsiness, we will follow convention and refer to 'the group G' whenever the operation that makes the set into a group is clear from the context. We usually write the group operation as if it were multiplication: we write xy where we should, strictly, write $x \circ y$. The main exception to this rule will be where the group operation is called addition, in which case we write $x + y$.

There are several elementary consequences of these axioms that you will have seen when you were first introduced to groups. You may have noticed, for example, that the phrase 'an identity' in the second axiom has become 'the identity' in the third. This follows from the fact that a group can have only one identity. For ease of reference, the elementary consequences that you are expected to know are summarised in the following proposition.

Proposition 1.2 *Elementary consequences of the group axioms*

Let G be a group.

(a) **Uniqueness of identity**

The identity element of G is unique.

(b) **Uniqueness of inverses**

Let a be an element of G. Then the inverse of a is unique.

(c) **Left cancellation rule**

For any elements x, y and a of G,

$$ax = ay \quad \text{implies} \quad x = y.$$

(d) **Right cancellation rule**

For any elements x, y and a of G,

$$xa = ya \quad \text{implies} \quad x = y.$$

(e) **Inverse of a product**

For any elements x and y of G, the inverse of the product xy is $y^{-1}x^{-1}$.

Proposition 1.2(e) says that

$$(xy)^{-1} = y^{-1}x^{-1}.$$

The fact that there is a reversal of order in the inverse of a product may seem strange initially. However, consider the process of putting on your shoes and socks. The reverse process (*inverse*) clearly involves taking off your shoes before taking off your socks!

Worked Exercise 1.3

Show that the set of the integers with addition, $(\mathbb{Z}, +)$, is a group.

Solution

We check the axioms.

Closure The sum of two integers, positive or negative, is another integer.

Identity The integer 0 is the identity element for addition: for any integer x,

$$x + 0 = x = 0 + x.$$

Inverses The inverse of an integer x is the integer $-x$, because $x + (-x) = 0 = (-x) + x$ and 0 is the identity element of $\mathbb{Z}$.

Associativity From what we know about addition, it is the case that $(x + y) + z = x + (y + z)$ for all choices of integers x, y and z.

You will know from your previous studies that the sets of numbers $(\mathbb{Q}, +), (\mathbb{Q}\backslash\{0\}, \times), (\mathbb{R}, +), (\mathbb{R}\backslash\{0\}, \times), (\mathbb{C}, +), (\mathbb{C}\backslash\{0\}, \times)$ are groups. We will not show the details here.

Exercise 1.1

Check that each of the following sets, with the given operation, forms a group. For each example, you should specify the identity of the group and how to find an inverse for each element. You may assume that matrix multiplication is associative.

(a) Set: all 2×2 matrices with real numbers as entries and non-zero determinant.

Operation: matrix multiplication.

(b) Set: all 2×2 matrices of the form

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \quad a \in \mathbb{Z}.$$

Operation: matrix multiplication.

The group in Exercise 1.1(a) is an important example called the **general linear group** $\mathrm{GL}(2, \mathbb{R})$. The word 'linear' is used because matrices represent linear transformations between vector spaces. The 2 indicates the size of the matrices, and the $\mathbb{R}$ indicates that the entries are real numbers.

Exercise 1.2

Let G be a group, and let x and y be elements of G.

(a) Use the uniqueness of inverse elements to prove Proposition 1.2(e): the inverse of the product xy is $y^{-1}x^{-1}$.

(b) Show that $\left(x^{-1}\right)^{-1} = x$.

Proposition 1.2(e) can be generalised to the inverse of a product of any number of elements, namely

$$(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}.$$

This result is proved by mathematical induction. Even though the proof is not included here, we will use the result when required.

Exercise 1.3

Let G be a group with identity e and let x be an element of G.

(a) Show that if g is an element of G such that $gx = x$, then $g = e$. In other words, show that if g behaves like a left identity for the particular element x of G, then g is the identity of the group.

(b) State and prove the corresponding result with 'left' replaced by 'right'.

The solution to Exercise 1.3 provides us with a proof of the following proposition.

Proposition 1.4

Let G be a group with identity e and let x be an element of G.

If g is an element of G such that either $gx = x$ or $xg = x$, then $g = e$.

There is a similar result for inverses: if an element y of a group behaves like a right inverse for another element x, then y is *the* inverse of x.

Proposition 1.5

Let G be a group with identity e and let x be an element of G.

If $xy = e$ for some element y of G, then $y = x^{-1}$.

Proof We are given that $xy = e$. By the inverses axiom, $xx^{-1} = e$. Equating the two expressions for e gives $xy = xx^{-1}$. Using the left cancellation rule, we have $y = x^{-1}$. ■

An alternative proof for Proposition 1.5 involves multiplying both sides of the equation $xy = e$ on the left by the element x^{-1}.

Exercise 1.4

Let G be a group with identity e and let x be an element of G. Show that if an element y of a group G behaves like a left inverse for the element x, that is $yx = e$, then $y = x^{-1}$.

Proposition 1.5 and Exercise 1.4 tell us that if y behaves as either a left inverse or a right inverse of x, then y is *the* inverse of x.

Proposition 1.6

Let G be a group with identity e and let x be an element of G.

If y is an element of G such that either $yx = e$ or $xy = e$, then $y = x^{-1}$.

Before looking at some further examples of groups, we want to say two things about associativity.

Firstly, the associativity axiom guarantees that the two ways of bracketing a combination of *three* elements leads to the same result. It says nothing directly about expressions such as

$$x_1 \circ x_2 \circ \cdots \circ x_n.$$

Fortunately, it is possible to prove (by induction) that all ways of bracketing such an expression lead to the same result. The proof is more involved than illuminating, and so we do not give it. We will assume the result and write such expressions without brackets, doing any specific calculation by combining pairs in the most convenient way.

Proposition 1.7 *Generalised associativity rule*

Let G be a group and n be a positive integer. Then the product of n elements of G, *taken in a fixed order*, is the same no matter which way the product is calculated.

Secondly, a 'first principles' proof that associativity holds in a particular example is usually the messiest part of verifying that an example is a group. Fortunately, for very large classes of groups, including most of those considered in this module, there are quicker ways to prove associativity.

For example, the 2×2 matrices in $\mathrm{GL}(2, \mathbb{R})$ can be thought of as functions from the plane $\mathbb{R}^2$ to itself. The group operation in this case is, effectively, composition of functions. Now, as you may remember from your previous studies, composition of functions is always associative. This fact removes the need to check associativity in any example where the elements are

matrices and the operation is matrix multiplication. We will use this principle freely in the rest of the module.

We can further reduce the number of cases where a check is necessary by observing that if an operation on a given set is associative, then associativity is inherited by any subset that is closed under the operation.

1.2 Permutations

An important example of a whole class of groups is provided by the **symmetric groups** S_n, where n is a positive integer.

The set S_n is defined as the set of all functions

$$f : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

A bijection is also known as a **one–one correspondence**.

where f is a *bijection*, with composition of functions as the operation. The elements of S_n are called **permutations**, and each S_n is an example of a **permutation group**.

We remind you of the notation used for permutations by giving a specific example. In S_4, the **two-line notation**

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

represents the permutation $\begin{array}{ccc} 1 & \mapsto & 4 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \\ 4 & \mapsto & 1\,. \end{array}$

For this permutation, $1 \mapsto 4 \mapsto 1$ and $2 \mapsto 3 \mapsto 2$, so the permutation can be written in **cycles** as

$$(1\,4)(2\,3).$$

The cycles $(1\,4)$ and $(2\,3)$ are **disjoint**, that is, they contain no numbers in common. Any permutation can be broken down into disjoint cycles. A permutation written as a composite of disjoint cycles is said to be in **cycle form**.

Moreover, any cycle $(a_1\ a_2\ \ldots\ a_n)$ can be expressed as a composite of cycles of length 2 (also called **transpositions**), as follows:

$$(a_1\ a_2\ \ldots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})(a_1\ a_{n-2}) \cdots (a_1\ a_3)(a_1\ a_2).$$

It follows that any permutation can be expressed as a composite of transpositions. This may be done in several different ways, but for a given permutation the number of transpositions appearing in a decomposition is always either even or odd. Thus, a permutation is said to be **even** if it can be expressed as the composite of an even number of transpositions, and **odd** otherwise.

We will often refer to the composition of permutations as a *product*; that is, we will speak about the product of two cycles, or the product of two permutations, to mean their composition.

Exercise 1.5

(a) Evaluate the following product in S_5, leaving your answer in two-line notation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

Hint: remember that the permutation on the right must be applied first.

(b) Write the following element of S_5 in cycle form.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

(c) Write the following product in S_6 in cycle form.

$(1\,6\,3)(2\,5\,4)(1\,3\,5\,6\,2)$

Another class of permutation groups are the **alternating groups** A_n, where n is a positive integer. The elements of A_n are all the even permutations in S_n.

1.3 Symmetries of figures

A rich collection of examples of groups comes from considering symmetries of geometric objects. The first example of these that we will consider is shown in Figure 1.1. This group consists of the isometries of the plane that leave the rectangle fixed as a whole; that is, those isometries that map the set of points forming the rectangle onto itself, where we regard a rectangle as consisting of just its boundary. Note that we have not said the isometries fix each point of the rectangle. For example, the isometry given by a half-turn (i.e. a turn through π, denoted by r_π in Figure 1.1) about the centre O of the rectangle leaves no point of the rectangle in its original position (except O itself), but it does fix the whole rectangle and so is a symmetry of the rectangle.

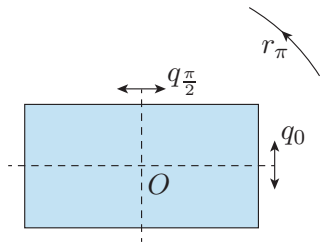


Figure 1.1 Symmetries of a rectangle

Although you are probably familiar with the symmetries of the rectangle, it will be useful to recall how we can be sure exactly which isometries belong to this group. To do so, we use an approach that will be useful in more complicated examples. The approach is based on certain consequences of the defining property of isometries: that they preserve distance.

We find all the symmetries of the rectangle in two stages. Firstly, we decide what isometries might possibly occur as symmetries. Secondly, we show that all such possibilities are realised.

The strategy adopted here is a very useful one. We find an upper limit to the number of isometries in a symmetry group and then show that we can find that many different symmetries.

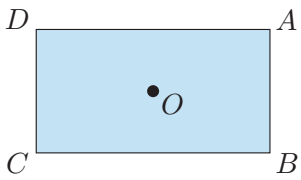


Figure 1.2 Rectangle with labelled corners

Label the corners of the rectangle A, B, C, D as in Figure 1.2. An isometry must map the corner A to itself or one of the other three corners. Once the image of A is fixed, it must be opposite to the image of C under the isometry. Moreover, since the rectangle is not square and an isometry preserves distances, the image of B must be at the other end of the shorter side from the image of A. Thus the choice of where A maps to determines the isometry. Therefore there are at most four symmetries.

We can indeed find four different symmetries of the rectangle. The identity mapping is one, with A mapping to A; a half-turn about the point O, with A mapping to C, is another; reflection in the horizontal axis of symmetry, with A mapping to B, gives a third; reflection in the vertical axis of symmetry, with A mapping to D, gives the last. These are all different since A maps to a different corner in each case. Since we know that there are at most four symmetries, we know that we have them all.

The *Cayley table* for a group is a table describing the result of applying the group operation to every pair of elements of the group.

If we denote the symmetries (in the order described above) as e, r, h and v, then we can construct a Cayley table where the operation is composition of the symmetries.

$\circ$	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

By choosing an origin at the centre of the rectangle and coordinate axes parallel to the sides of the rectangle, we can represent the four symmetries e, r, h and v using the following functions from $\mathbb{R}^2$ to $\mathbb{R}^2$:

$$e((x,y)) = (x,y),$$
$$r((x,y)) = (-x,-y),$$
$$h((x,y)) = (x,-y),$$
$$v((x,y)) = (-x,y).$$

The functions e, r, h and v in turn can be represented by the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

respectively. Thus we have a second representation of the group of symmetries of the rectangle, this time as a group of matrices under multiplication.

There is a third representation of this group, which can be obtained if we number the corners of the rectangle 1 to 4, as in Figure 1.3. Since corners map to corners, each symmetry corresponds to a permutation of the set $\{1,2,3,4\}$, that is to an element of S_4, as follows:

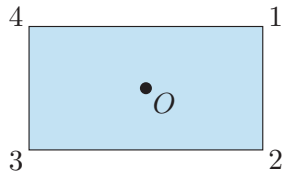


Figure 1.3 Rectangle with numbered corners

$$e \text{ corresponds to } \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},$$

$$r \text{ corresponds to } \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = (1\,3)(2\,4),$$

$$h \text{ corresponds to } \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = (1\,2)(3\,4),$$

$$v \text{ corresponds to } \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = (1\,4)(2\,3).$$

This group of four permutations forms a *subgroup* of S_4, which itself has 24 elements.

These three representations illustrate an important point: a group may have several different but equivalent representations. Here, then, we can consider that we have three concrete examples of groups all essentially the same as the group of symmetries of a rectangle. Thus, depending on the context, we may regard any one of these groups as *the* group of symmetries of a rectangle. The sense in which these representations are 'equivalent' and the groups are 'essentially the same' will be made more precise in Section 4.

More generally, if we have a subset X of the plane, $\mathbb{R}^2$, then the isometries of $\mathbb{R}^2$ that map X onto itself form a group called the **symmetry group** of X. We will denote the symmetry group of X by $\Gamma(X)$. Thus we denote the **symmetry group of a rectangle** by $\Gamma(\rule{1em}{0.6em})$. Where the subset X is large, or complicated, the $\Gamma(\cdot)$ notation can become unwieldy, and in such cases we introduce more convenient notation.

Or, more generally still, $\mathbb{R}^n$.

The group of all symmetries of the plane $\mathbb{R}^2$, that is where $X = \mathbb{R}^2$, is known as the **orthogonal group** and denoted by $\mathrm{O}(2,\mathbb{R})$. Elements of $\mathrm{O}(2,\mathbb{R})$ can be represented by certain 2×2 real matrices with determinant ± 1. The group of all rotations of the plane, whose elements can be represented by certain 2×2 real matrices with determinant 1, is known as the **special orthogonal group** and denoted by $\mathrm{SO}(2,\mathbb{R})$.

In both cases the group operation is matrix multiplication.

The symmetries of a regular hexagon form a group known as the **symmetry group of the regular hexagon**, which we will refer to as D_6. You may have already met this group in your previous studies under the rather more suggestive names of $\Gamma(\hexagon)$ and $S(\text{Hexagon})$. However, there are two other names in fairly common use. One is our preferred notation D_6, where the suffix denotes the number of *sides* of the *polygon*; the other is D_{12}, where the suffix indicates the number of *elements* in the *group*. The label D is for *dihedral*. There is a whole family of dihedral groups, one for each regular polygon. You have probably also met D_4, the **symmetry group of a square**, perhaps with the name $S(\square)$ or $\Gamma(\square)$.

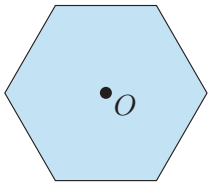


Figure 1.4 A regular hexagon with centre O

Exercise 1.6

(a) Explain why there are at most 12 symmetries of a regular hexagon (Figure 1.4) and how all 12 can be realised.

(b) In D_6 let r denote anticlockwise rotation through $\frac{\pi}{3}$ and s denote a reflection in an axis of symmetry. Show that $r^6 = e$ and $sr = r^5 s$.

Equalities that hold among elements of a group, such as the ones you found in Exercise 1.6(b), are known as **relations**.

1.4 Cyclic groups

Cyclic groups can be regarded as groups of symmetries of figures such as the one shown in Figure 1.5, where we use the curved 'arms' to remove any reflections.

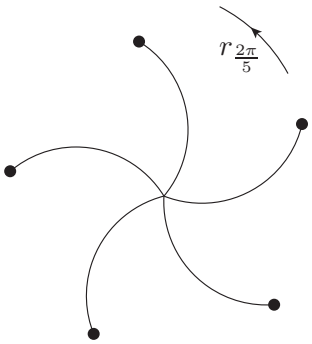


Figure 1.5 A figure whose symmetries give a cyclic group

Definition 1.8 *Cyclic group*

A group G is **cyclic** if every element has the form g^n for some element g in G. Such an element g is called a **generator** of the group.

A generator for the group of symmetries of the figure in Figure 1.5 is the anticlockwise rotation of $\frac{2\pi}{5}$ about the centre of the figure, denoted by $r_{\frac{2\pi}{5}}$.

The notation $\langle g \rangle$ represents the cyclic group generated by g.

When we considered the symmetries of a rectangle, we represented the symmetries as a set of permutations by labelling the vertices of the rectangle. We can do the same here: if we label each 'arm' in the figure with a number from 1 to 5, we can represent the rotations as permutations (Figure 1.6).

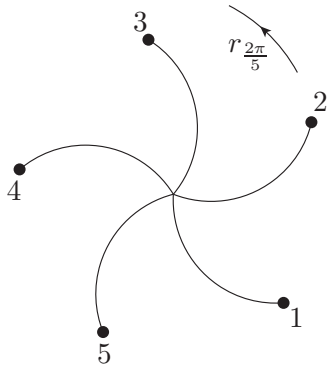


Figure 1.6 Representing rotations as permutations

The labelling in Figure 1.6 gives the permutation representation shown in Table 1.1.

Table 1.1 Permutation representation using labelling from Figure 1.6

Rotation	Permutation representation
Rotation through $\frac{2\pi}{5}$	$(1\,2\,3\,4\,5)$
Rotation through $\frac{4\pi}{5}$	$(1\,3\,5\,2\,4) = (1\,2\,3\,4\,5)^2$
Rotation through $\frac{6\pi}{5}$	$(1\,4\,2\,5\,3) = (1\,2\,3\,4\,5)^3$
Rotation through $\frac{8\pi}{5}$	$(1\,5\,4\,3\,2) = (1\,2\,3\,4\,5)^4$
Rotation through 0	$(1)(2)(3)(4)(5) = e = (1\,2\,3\,4\,5)^5$

In this representation a generator is $(1\,2\,3\,4\,5)$. We talk about *a* generator, not *the* generator, because the generator of a cyclic group is not necessarily

unique. For example, if we let $g = r_{\frac{2\pi}{5}}$ then $g^5 = e$, the rotation through zero – that is, the identity of the group – and the symmetries of the figure can be given as $\{g, g^2, g^3, g^4, e\}$. They can also be given as

$$\{g^2, (g^2)^2 = g^4, (g^2)^3 = g, (g^2)^4 = g^3, (g^2)^5 = e\},$$

and so g^2 also is a generator of the group. In other words,

$$\langle r_{\frac{2\pi}{5}} \rangle = \langle r_{\frac{4\pi}{5}} \rangle.$$

The usual rules of indices apply.

Recall that a group is **abelian** if the binary operation is commutative. That is, G is an abelian group if

$$a \circ b = b \circ a, \quad \text{for all } a, b \in G.$$

The term *abelian* is in honour of the Norwegian mathematician Niels Henrik Abel (1802–1829).

Cyclic groups are abelian, as you are asked to verify in the next exercise.

Exercise 1.7

Prove that every cyclic group is abelian.

For an abelian group G, we often write the group operation additively, using $+$, so commutativity is expressed as

$$x + y = y + x \text{ for all } x, y \in G.$$

Before we consider such groups, a few words are in order about notation for groups written additively.

When n is a positive integer, the general symbol x^n means n copies of x combined using the group operation. In additive notation this becomes

$$\overbrace{x + \cdots + x}^{n \text{ copies}},$$

which we write as nx rather than x^n.

When $+$ is used for the group operation, the identity is written as 0 and the inverse of x as $-x$.

1.5 Groups from modular arithmetic

Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with the binary operation addition modulo 6. It is not difficult to see that this set is closed under this operation, that the operation is associative and that the identity is 0. The inverse of each element $a \in \mathbb{Z}_6$ is the standard representative of $-a \pmod 6$ and so a member of the set. Hence $\mathbb{Z}_6$ with addition modulo 6 is a group. From now on we will use $+_n$ to represent addition modulo n.

Each element a of $\mathbb{Z}_6$ can be obtained by adding 1 to itself $a - 1$ times – that is, adding a ones together. Thus $\mathbb{Z}_6$ is a cyclic group generated by 1.

More generally, the set $\mathbb{Z}_n$ with addition modulo n forms a group for any integer $n > 1$. For these groups, we use either the notation $\mathbb{Z}_n$ or the

notation $(\mathbb{Z}_n, +_n)$, depending on whether we want to specify the operation. For each $n \in \mathbb{N}$, the group $(\mathbb{Z}_n, +_n)$ is cyclic with generator 1.

Exercise 1.8

Write down all the generators of $\mathbb{Z}_6$.

In the solution to Exercise 1.8, you may have noticed that the generators m of $\mathbb{Z}_6$ are precisely those for which $\text{hcf}(m, 6) = 1$. This is an instance of a general property of the cyclic group $\mathbb{Z}_n$: an element m of $\mathbb{Z}_n$ is a generator if $\text{hcf}(m, n) = 1$.

We can also find some cyclic groups by considering modular *multiplication*, as in the example below. From now on, multiplication modulo n will be denoted by $\times_n$, and the set $\mathbb{Z}_n \setminus \{0\}$ by $\mathbb{Z}_n^*$.

The notation $\mathbb{Z}_n \setminus \{0\}$ indicates the set $\mathbb{Z}_n$ without the element 0. This is also sometimes denoted by $\mathbb{Z}_n - \{0\}$.

Example 1.9 *The cyclic group* $(\mathbb{Z}_5^*, \times_5)$

Let $G = \mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Then $(G, \times_5)$ is a cyclic group generated by 2 (or 3).

Closure and associativity follow from the rules of modular multiplication.

The identity is 1.

We see that the inverse of 2 is 3, the inverse of 3 is 2 and 4 is self-inverse:

$$2 \times_5 3 \equiv 1 \text{ since } 2 \times 3 = 6 \equiv 1 \,(\text{mod } 5),$$
$$4 \times_5 4 \equiv 1 \text{ since } 4 \times 4 = 16 \equiv 1 \,(\text{mod } 5).$$

As $2^2 \equiv 4 \,(\text{mod } 5), 2^3 \equiv 3 \,(\text{mod } 5)$ and $2^4 \equiv 1 \,(\text{mod } 5)$, the group is cyclic and generated by 2.

It is often the case that $\mathbb{Z}_n^*$ is not a group under modular multiplication, since the operation is not closed. For example, in $\mathbb{Z}_6^*$ we have that $3 \times_6 2 \equiv 0$.

Exercise 1.9

Show that $(\mathbb{Z}_5^*, \times_5)$ is not generated by 4.

2 Subgroups and cosets

The concept of a subgroup, which you probably met in your previous studies, arises when a group H is contained within a larger group G in such a way that the group operation on H is induced by that on G. This section revises the definition and main properties of subgroups. It also considers how any subgroup gives rise to a partition of the host group into

blocks called *cosets*, and how this notion is pivotal in the proof of the group-theoretic Lagrange's Theorem, a result on the possible sizes of the subgroups of a group.

2.1 Subgroups

We start this section by reminding you of the definition of a subgroup.

Definition 2.1 *Subgroup*

A subset H of the underlying set of a group G is a **subgroup** of G if it is itself a group under the group operation of G.

We use the notation

$$H \leq G$$

to denote that H is a subgroup of G.

Since H is a subset of G and the group operation is associative in G, the operation is also associative in H, provided H is closed. Thus, checking the group axioms for a subset H of a group G reduces to the following.

Proposition 2.2 *Subgroup conditions*

If G is a group with binary operation $\circ$ and H is a subset of the underlying set of G, then H is a subgroup of G (with binary operation $\circ$) if all the following conditions are satisfied.

SG1 Closure For all pairs x, y of elements in H, $x \circ y$ is also in H.

SG2 Identity The identity element e of G is in H.

SG3 Inverses For each element x in H, the inverse element x^{-1} in G is also in H.

In particular, the identity of H is the same as the identity of G and inverses of elements in H are the same as their inverses in G.

We will often refer to conditions SG1, SG2 and SG3 as the *subgroup axioms*.

It is worth observing that in order to check for closure, we need only to check pairs of elements x, y where neither element is equal to the identity. This is because if $x, y \in H$ and $x = e$, then $xy = ey = y \in H$. Similarly, if $y = e$, then $xy = x \in H$.

Exercise 2.1

Prove that the set $H = \{e, (1\,2\,3), (1\,3\,2)\}$ is a subgroup of the permutation group S_3.

The following proposition reminds you that in any group there are at least two subgroups.

Proposition 2.3

Let G be a group. Then:

(a) if e is the identity, then $\{e\}$ is a subgroup of G

(b) G is a subgroup of G.

Proof The subgroup conditions are satisfied in both cases. ■

The subgroup $\{e\}$ is referred to as the **trivial subgroup**. In some texts, the term **proper subgroup** is used for a subgroup that is not the whole group.

Exercise 2.2

Write down all the subgroups of $\mathbb{Z}_6$.

There are several alternative ways of testing whether a particular subset of a group is a subgroup. The one we give in the following proposition is useful because it is somewhat simpler to apply than checking the three conditions in Proposition 2.2.

Proposition 2.4 *Subgroup criterion*

Let G be a group and H be a subset of the underlying set of G. Then H is a subgroup of G if, and only if, it satisfies the following two properties:

(a) H is non-empty

(b) $x, y \in H$ implies $x^{-1}y \in H$.

Proof We start by proving the 'if' part of the statement of the theorem: we are given that H is a non-empty subset of G and that, if x and y are in H, then $x^{-1}y$ is in H. We have to show that H is a subgroup of G; in other words, that H satisfies the three subgroup axioms. It turns out that the easiest way of proving the axioms is not in the order in which they appear in Proposition 2.2, but as follows.

Identity By property (a), H is non-empty. Therefore there exists some element x in H. By property (b), if x and y are in H, then $x^{-1}y$ is in H. The special case $y = x$ shows that $x^{-1}x = e$ is in H. Thus, H satisfies the identity axiom.

Inverses If x is in H then, by the identity axiom (already verified), both x and e are in H. Then, by property (b), the inverse $x^{-1}e = x^{-1}$ is in H, so H satisfies the inverses axiom.

Closure Let x and y be elements of H. By the inverses axiom (already verified), x^{-1} is an element of H. Therefore x^{-1} and y are both in H. So, by property (b), the product $\left(x^{-1}\right)^{-1} y = xy$ is in H. Therefore H satisfies the closure axiom.

This concludes the proof of the 'if' part of the theorem.

For the 'only if' part, we need to prove that if H is a subgroup of G, then H has the two properties (a) and (b). You are asked to prove this in Exercise 2.3 below. ■

Exercise 2.3

Let G be a group and H be a subgroup of G. Prove that H is a non-empty subset of G and that, if x and y are elements of H, then so is $x^{-1}y$.

The following exercise asks you to prove an alternative subgroup criterion.

Exercise 2.4

Let G be a group and H be a subset of the underlying set of G. Prove that H is a subgroup of G if, and only if, it satisfies the following two properties:

(a) H is non-empty, i.e. $H \neq \emptyset$

(b) $x, y \in H$ implies $xy^{-1} \in H$.

We now have two alternative tests to use to decide whether a subset of a group is a subgroup. We state them in additive notation before looking at an example.

Proposition 2.5 *Subgroup criteria (additive notation)*

1. A subset H of a group G, written using additive notation, is a subgroup if, and only if, it satisfies the following conditions:
   (a) H is non-empty
   (b) $x, y \in H$ implies $-x + y \in H$.
2. A subset H of an additive group G is a subgroup if, and only if, it satisfies the following conditions:
   (a) H is non-empty
   (b) $x, y \in H$ implies $x - y \in H$.

The second subgroup criterion looks more natural for abelian groups with additive notation.

As an example, we use criterion 2 of Proposition 2.5 to prove that $(2\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$.

Remember that $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$.

Firstly, $2\mathbb{Z}$ is non-empty since, for example, $0 = 2 \times 0$ is in $2\mathbb{Z}$.

Secondly, let x and y be two elements of $2\mathbb{Z}$. By the definition of $2\mathbb{Z}$, there exist integers m and n such that $x = 2m$ and $y = 2n$. So

$$x - y = 2m - 2n = 2(m - n).$$

However, $m - n$ is an element of $\mathbb{Z}$. Therefore $2(m - n)$ is an element of $2\mathbb{Z}$.

This completes the proof.

Exercise 2.5

Let G be a group and let H be a subgroup of G.

(a) Show that if K is a subgroup of H then K is a subgroup of G.

(b) Show that if K is a subgroup of G and the underlying set of K is a subset of the underlying set of H, then K is a subgroup of H.

The following result is a further consequence of Proposition 2.4.

Proposition 2.6

Let G be a group and H_1 and H_2 be subgroups of G. Then the intersection $H_1 \cap H_2$ is a subgroup of G, and also a subgroup of both H_1 and H_2.

Proof Firstly, since H_1 and H_2 are subgroups of G, each contains the identity e of G. Therefore e is an element of $H_1 \cap H_2$, and so $H_1 \cap H_2$ is non-empty.

Secondly, if x and y are in $H_1 \cap H_2$, then x and y must be in both H_1 and H_2. By Proposition 2.4, the product $x^{-1}y$ is in both H_1 and H_2. Therefore $x^{-1}y$ is in $H_1 \cap H_2$.

We have verified that the intersection $H_1 \cap H_2$ has the two properties in Proposition 2.4, and so $H_1 \cap H_2 \leq G$.

Since, by definition, $H_1 \cap H_2$ is a subset of both of the subgroups H_1 and H_2, and since, as we have proved, it is a subgroup of G, Exercise 2.5 gives $H_1 \cap H_2 \leq H_1$ and $H_1 \cap H_2 \leq H_2$. ■

Proposition 2.6 generalises to any non-empty collection of subgroups of a group G. For a finite collection, the proof is almost identical to that above. The result is still true for infinite collections of subgroups, though the proof in this case is a little more complicated because of some notational difficulties. Neither proof is given here, but since we will use this result later, we state it in full generality.

Proposition 2.7

Let G be a group. The intersection of any non-empty collection of subgroups of G is a subgroup both of G and of each of the subgroups in the collection.

A natural question that arises now is whether a union of subgroups of a given group is also a subgroup. The answer is no, as the following exercise shows.

It is a fact of life that intersections are nearly always much nicer than unions. This is because intersections share common properties rather than lumping everything together.

Exercise 2.6

Give an example of a group with two subgroups whose union is not a subgroup.

Hint: consider the group $\mathbb{Z}_6$.

Some, but not all, properties of a group are inherited by its subgroups. Here is an example.

Exercise 2.7

Prove that all subgroups of abelian groups are abelian.

2.2 Cosets and Lagrange's Theorem

In your previous mathematical studies you should have encountered the *cosets* of a subgroup in a given group. We remind you of the definition of a *left* coset.

Definition 2.8 *Left coset*

Let G be a group, H be a subgroup of G and a be an element of G. Then the subset

$$aH = \{ah : h \in H\}$$

is called the **left coset** of H by a.

More generally, for any two subsets A and B of G, the set defined by $AB = \{ab : a \in A, b \in B\}$ is said to be the **product** of A and B. So, with this convention, the left coset aH is defined to be the product $\{a\}H$.

Exercise 2.8

Write down all the left cosets of the subgroup $\{e, (1\,2)\}$ in the permutation group S_3.

Example 2.9 *Cosets of S_3*

In the solution to Exercise 2.8, with $G = S_3$ and $H = \{e, (1\,2)\}$, we saw that the two left cosets eH and $(1\,2)H$ are the same, as are $(1\,3)H$ and $(1\,2\,3)H$, and indeed $(2\,3)H$ and $(1\,3\,2)H$.

So, for different elements a and b of G, the left cosets aH and bH may turn out to be the same.

Moreover, in this example the union of the distinct cosets $\{e, (1\,2)\}$, $\{(1\,3), (1\,2\,3)\}$ and $\{(2\,3), (1\,3\,2)\}$ is the whole group. The cosets are also disjoint, that is, the intersection of any two is the empty set. Furthermore, each coset has the same number of elements.

These results generalise and lead to Lagrange's Theorem.

The conditions under which two cosets are the same are important in the proof of the group-theoretic Lagrange Theorem, which we will see shortly.

In Example 2.9, a coset aH is equal to H precisely when the element a is in H. The following proposition shows that this result holds in general.

Proposition 2.10

Let G be a group and H be a subgroup of G. Then $aH = H$ if, and only if, a is an element of H.

Proof Assume that a is an element of the subgroup H. We want to prove that $aH = H$.

Firstly we show that $aH \subseteq H$. Let x be an element of aH. Then $x = ah$ for some h in H. Now a and h are elements of H and so, by the closure axiom, $ah = x$ is an element of H. Therefore aH is a subset of H.

Secondly we show that $H \subseteq aH$. Let y be an element of H. We may write $y = a(a^{-1}y)$. Since both a and y are in H, so is $a^{-1}y$, by Proposition 2.4. So $y = a(a^{-1}y)$ is an element of aH. Therefore H is a subset of aH.

Hence $aH = H$.

Conversely, assume that $aH = H$. We need to show that a is an element of H.

Since H is a subgroup, the identity element e is in H, therefore ae is in aH. However, $ae = a$ and $aH = H$, so a is in H. ■

Since $H = eH$, we have proved a result about the equality of the cosets aH and eH. A more general result concerning the equality of cosets is given in the following proposition.

Proposition 2.11

Let G be a group, H be a subgroup of G and a and b be elements of G. Then the left cosets aH and bH are equal if, and only if, $a^{-1}b \in H$.

Proof For the 'if' part of the statement, we assume that $a^{-1}b$ is an element of H, so $a^{-1}b = h$ for some h in H. To show that $aH = bH$, we must show that $aH \subseteq bH$ and that $bH \subseteq aH$.

Firstly we show that $aH \subseteq bH$. Let x be an element of aH, so that $x = ah_1$ for some h_1 in H. From $a^{-1}b = h$ we deduce (by multiplying both sides on the left by a and on the right by h^{-1}) that $a = bh^{-1}$, and so $x = bh^{-1}h_1$. But $h^{-1}h_1$ is an element of H, so x is an element of bH. Therefore aH is a subset of bH.

Secondly we show that $bH \subseteq aH$. Let y be an element of bH, so that $y = bh_2$ for some h_2 in H. From $a^{-1}b = h$ we deduce (by multiplying both sides on the left by a) that $b = ah$, and so $y = ahh_2$. But hh_2 is an element of H, so y is an element of aH. Therefore bH is a subset of aH.

You are asked to prove the 'only if' part of the proposition in Exercise 2.9. ■

Exercise 2.9

Let G be a group, H be a subgroup of G and a, b be elements of G such that $aH = bH$. Prove that $a^{-1}b$ is in H.

Since the statement $aH = bH$ in Proposition 2.11 is symmetric in a and b, we can deduce that, in addition,

$aH = bH$ if, and only if, $b^{-1}a \in H$.

Moreover, Proposition 2.11 allows us to prove the following useful fact.

Proposition 2.12

Let G be a group, H be a subgroup of G and a and b be elements of G. Then the left cosets aH and bH are either disjoint or equal.

Remember that two sets are *disjoint* if they have no elements in common.

Proof Since the cosets aH and bH are either disjoint or not, it suffices to show that if the left cosets aH and bH are not disjoint, then they are equal.

If aH and bH are not disjoint, there exists some element x that is in both aH and bH.

From the definition of left coset, this means that $x = ah_1$ and $x = bh_2$ for some h_1 and h_2 in H. Therefore $ah_1 = bh_2$. Multiplying on the left by a^{-1} and on the right by h_2^{-1} gives $a^{-1}b = h_1h_2^{-1}$. As $h_1h_2^{-1}$ is an element of H, Proposition 2.11 tells us that $aH = bH$. ■

Some conditions that are equivalent to the equality of two cosets are summarised in the next proposition.

Proposition 2.13

Let G be a group, H be a subgroup of G and a and b be elements of G. Then the following four statements are equivalent:

(a) $a^{-1}b \in H$

(b) $aH = bH$

(c) a and b are in the same left coset

(d) $b \in aH$.

Proof The equivalence (a) ⇔ (b) is given by Proposition 2.11.

Since $a \in aH$ and $b \in bH$, if $aH = bH$ then a and b are in the same coset. Conversely, if a and b are in the same coset, Proposition 2.12 gives $aH = bH$. We have established the equivalence (b) ⇔ (c).

Since $a \in aH$, the equivalence (c) ⇔ (d) follows from Proposition 2.12.

For (a) ⇒ (d), if $a^{-1}b \in H$ then $aH = bH$ by Proposition 2.11, and so $b \in aH$. Moreover, $b \in aH$ implies $aH = bH$, again by Proposition 2.12, and so $a^{-1}b \in H$ by Proposition 2.11. Thus (d) ⇒ (a). This concludes the proof. ■

Two sets A and B have the *same number of elements* if, and only if, there is a bijection from A to B. This is true even when the two sets are infinite, as the existence of such a bijection is the definition of 'having the same number of elements'.

The next exercise asks you to prove that all the cosets of a given subgroup of a group have the same number of elements. This result is pivotal in the proof of Lagrange's Theorem.

Exercise 2.10

Let G be a group, H be a subgroup of G and a and b be elements of G.

(a) Prove that the function $f : H \to aH$, $h \mapsto ah$ is a bijection, and hence that the sets H and aH have the same number of elements.

(b) Deduce that the left cosets aH and bH have the same number of elements.

Notation for functions is defined in detail in Book D, Chapter 13, Section 1.

We need two more definitions before we can state and prove Lagrange's Theorem.

Definition 2.14 *Finite and infinite groups*

A group is **finite** if its underlying set is finite, that is, it has a finite number of elements. If the underlying set is infinite, the group is an **infinite group**.

Definition 2.15 *Order of a group*

The **order** of a finite group G is the number of elements it contains, and it is denoted by $|G|$. An infinite group is said to have **infinite order**.

The notation $|G|$ corresponds to other uses of the modulus sign to denote size.

Recall that a collection of subsets $S_1, S_2, \ldots, S_k$ of a set S forms a **partition** of S if their union is the whole of S and every pair is disjoint. In this case, we sometimes also say that $S_1, S_2, \ldots, S_k$ *partition* S.

With this in mind, we are ready for Lagrange's Theorem. Note that we have already met a result called 'Lagrange's Theorem' in the context of polynomial congruences: Theorem 4.3 of Chapter 4. Both the theorem in Chapter 4 and Theorem 2.16 below are commonly referred to as 'Lagrange's Theorem', even though they are unrelated results. Mathematicians usually rely on the context to make it clear which of the two they are referring to. In this book, 'Lagrange's Theorem' will always denote the group-theoretic result that we are about to prove.

Theorem 2.16 *Lagrange's Theorem*

Let G be a finite group and H be a subgroup of G. Then the order of H divides the order of G, that is,

$|H|$ divides $|G|$.

Proof Since G has a finite number of elements, so does H.

Assume that the order of H is m.

Let a be any element of G. Then, since $a = ae$, we have that $a \in aH$. This shows that every element of G belongs to some coset of H. In particular, the union of the cosets of H in G is the whole of G. Moreover, by Proposition 2.12, the distinct left cosets of H are disjoint, hence they form a partition of G.

Assume that there are l such distinct cosets. By Exercise 2.10, we know that each of them has m elements. Then the total number of elements in G is lm, which shows that m divides the order of G. ■

Exercise 2.11

Write down all the subgroups of the permutation group S_3.

You can use Lagrange's Theorem to solve the following exercise.

Exercise 2.12

Let G be a group, and suppose that H and K are two finite subgroups whose orders are coprime. Show that $H \cap K = \{e\}$.

3 Normal subgroups and quotient groups

In the previous section we saw that a subgroup H of a group G partitions G into cosets. This section demonstrates that under certain conditions on H, the set of cosets is itself a group under a suitably defined operation. When the required conditions on H hold, we say that H is a *normal* subgroup, and the group of cosets is called the quotient group.

3.1 Normal subgroups

In the last section we considered only *left* cosets of a subgroup. The concept of *right* coset is entirely similar: given a subgroup H of a group G and an element a of G, we define the **right coset** of H by a as the set

$$Ha = \{ha : h \in H\}.$$

All the results in Subsection 2.2 that hold for left cosets also hold for right ones. For example, we have the following propositions.

Proposition 3.1

Let G be a group, H be a subgroup of G and a and b be elements of G. Then the right cosets Ha and Hb are equal if, and only if, $ab^{-1} \in H$.

The symmetry in a and b implies that an equivalent condition is $ba^{-1} \in H$.

Proposition 3.2

Let G be a group, H be a subgroup of G and a and b be elements of G. Then the right cosets Ha and Hb are either disjoint or equal.

The proofs of these results for right cosets are virtually identical to the ones already given for left cosets, and so we will not write them out.

Given a particular subgroup of a group, it may or may not be the case that a left coset is equal to the corresponding right coset.

Example 3.3 *Left and right cosets in S_3*

Let $G = S_3$ and $H = \{e, (1\,2)\}$. We saw in Exercise 2.8 that the left coset $(1\,2\,3)H$ is equal to $\{(1\,2\,3), (1\,3)\}$.

On the other hand, the right coset $H(1\,2\,3)$ is

$$\{(1\,2\,3), (1\,2)(1\,2\,3)\} = \{(1\,2\,3), (2\,3)\},$$

which is different from $(1\,2\,3)H$.

However, what is true is that there is a one–one correspondence between the left and right cosets of a given subgroup.

Exercise 3.1

Let G be a group and H be a subgroup of G. Show that the map ϕ from the set of left cosets of H to the set of right cosets of H defined by

$$\phi(aH) = Ha^{-1}, \quad \text{for } a \in G,$$

is well defined, one–one and onto.

ϕ is the Greek letter 'phi'.

In Exercise 3.1 we have shown the existence of a bijection between the left cosets and the right cosets of a given subgroup. One consequence is that the number of left cosets is the same as the number of right cosets. Thus we can give the following definition.

Definition 3.4 *Index of a subgroup*

Let G be a group, and H be a subgroup with finitely many cosets. Then the **index** of H in G is the number of left (or right) cosets of H in G.

In the proof of Lagrange's Theorem, we saw that the index of a subgroup H in a finite group G is the quotient $\frac{|G|}{|H|}$. We will make use of this result so often that it is worth highlighting as a proposition.

Proposition 3.5

Let G be a finite group and let H be a subgroup of G. Then the index of H in G is $\frac{|G|}{|H|}$.

Although the number of right cosets of a subgroup is the same as the number of left cosets, we have seen that, in general, if a is an element of G, the left coset aH is different from the right coset Ha. We now consider the special case of a subgroup H where aH and Ha are the same for all $a \in G$.

Definition 3.6 *Normal subgroup*

Let H be a subgroup of a group G. Then H is a **normal subgroup** of G if

$$aH = Ha$$

for every $a \in G$.

Note that we have *not* said that $ah = ha$ for all $a \in G$ and $h \in H$ individually, but just that the sets aH and Ha are the same.

Exercise 3.2

(a) Prove that in any group G, the subgroups $\{e\}$ and G are both normal subgroups.

(b) Prove that all subgroups of an abelian group are normal.

Verifying the normality condition in Definition 3.6 is not usually the most convenient way to check whether a certain subgroup is normal. There are several results of the form

the subgroup H is normal if, and only if, H has some property

where the property is easier to check than the definition. Two of these results are given in the following proposition.

Proposition 3.7

Let H be a subgroup of the group G. Then:

(a) H is a normal subgroup if, and only if, $aHa^{-1} \subseteq H$ for each a in G, where $aHa^{-1} = \{aha^{-1} : h \in H\}$.

(b) H is a normal subgroup if, and only if, the set of left cosets of H is equal to the set of right cosets of H.

Proof

(a) Assume that H is a normal subgroup of G. We want to show that $aHa^{-1} \subseteq H$ for each element a of G.

If x is in aHa^{-1}, then $x = ah_1a^{-1}$ for some $h_1 \in H$.

But ah_1 is in aH, which is equal to Ha. Therefore $ah_1 = h_2a$ for some h_2 in H. So

$$x = ah_1a^{-1} = h_2aa^{-1} = h_2 \in H.$$

Therefore $aHa^{-1} \subseteq H$.

Conversely, suppose that $aHa^{-1} \subseteq H$ for each element a of G. We want to show that $aH = Ha$.

We begin by showing that $aH \subseteq Ha$. Let x be in aH, so that $x = ah_1$ for some h_1 in H. The element $xa^{-1} = ah_1a^{-1}$ is in aHa^{-1}. Since aHa^{-1} is a subset of H, it follows that xa^{-1} is in H. Therefore $xa^{-1} = h_2$ for some h_2 in H. Hence $x = h_2a$, which is in Ha, and so aH is a subset of Ha.

We now show that $Ha \subseteq aH$. Let x be in Ha, so that $x = h_1a$ for some h_1 in H. We wish to show that x is in aH, that is, $x = ah$ for some $h \in H$. So we need to show that $a^{-1}x \in H$.

Now $a^{-1}x = a^{-1}h_1a$, and if we rewrite this as

$$a^{-1}h_1a = a^{-1}h_1(a^{-1})^{-1},$$

we see that $a^{-1}x$ is an element of the set $a^{-1}H(a^{-1})^{-1}$.

But the condition $aHa^{-1} \subseteq H$ holds for any $a \in G$, hence also for a^{-1}. So $a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H$. Therefore $a^{-1}x = h_2$ for some $h_2 \in H$, and so $x = ah_2$, which is an element of aH. This shows that Ha is a subset of aH. Therefore $aH = Ha$.

(b) If H is a normal subgroup of G, Definition 3.6 implies immediately that the set of left cosets is equal to the set of right cosets, since $aH = Ha$ for all $a \in G$.

Conversely, assume that the set of left cosets is equal to the set of right cosets. Let $a \in G$ and consider the right coset Ha. By our assumption, $Ha = bH$ for some $b \in G$. Thus $a \in bH$ and we have $bH = aH$ by Proposition 2.13. Thus $Ha = aH$ for all $a \in G$, and so H is normal in G. ■

Exercise 3.3

(a) Show that $H = \{e, (1\,2\,3), (1\,3\,2)\}$ is a normal subgroup of the permutation group S_3.

(b) Let H be a subgroup of a group G. Prove that if the index of H in G is 2, then H is a normal subgroup.

(c) Show that the intersection of a collection of normal subgroups of a group G is again a normal subgroup of G.

Given a group G and a subset S of G, there is a unique smallest normal subgroup of G that contains S.

Theorem 3.8

Let G be a group and S be a subset of (the underlying set of) G.

Then there exists a normal subgroup N of G that contains S, and such that for any other normal subgroup M of G containing S, $N \subseteq M$.

Proof Consider the collection of all normal subgroups containing the set S. The collection is non-empty, since G is a normal subgroup containing S. Let N be the intersection of this collection.

By the solution to Exercise 3.3(c), N is a normal subgroup of G. Moreover, N contains S by definition of intersection.

By the method of construction, N is the smallest such normal subgroup. ■

Proposition 3.7(a) might have reminded you about the notion of *conjugacy* in groups. Before giving the key definitions and results concerning conjugacy, we ask you to work through the following exercise.

Exercise 3.4

Let G be a group, H be a subgroup of G and let $g \in G$. Show that the set $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G.

We are now ready for the definitions of conjugate elements and conjugate subgroups.

Definition 3.9 *Conjugate elements and subgroups*

Let G be a group and let a and b be elements of G.

(a) The elements a and b are said to be **conjugate elements** in G if there exists $g \in G$ such that $gag^{-1} = b$.

(b) The **conjugacy class** of a in G is the set of elements conjugate to a, that is, the set

$$\mathrm{Conj}_G(a) = \{gag^{-1} : g \in G\}.$$

(c) Two subgroups H and K in G are said to be **conjugate subgroups** in G if there exists $g \in G$ such that $gHg^{-1} = K$.

The third part of Definition 3.9 allows us to formulate another criterion to decide whether a given subgroup is normal.

Proposition 3.10

Let G be a group. Then a subgroup N is normal in G if, and only if, N has no conjugate subgroups apart from N.

Proof Let N be normal in G and let $g \in G$. Then $gNg^{-1} \subseteq N$ by Proposition 3.7. Since $N \subseteq gNg^{-1}$, we have $N = gNg^{-1}$ and so N is the only subgroup of G conjugate to N.

Conversely, suppose that N is the only subgroup conjugate to N. Then $gNg^{-1} = N$ for all $g \in G$, so N is normal by Proposition 3.7. ■

The following exercise gives an important property of conjugacy of group elements.

Exercise 3.5

Define a relation $\sim$ on the elements of a group G by

$a \sim b$ if, and only if, a is conjugate to b.

Show that $\sim$ is an equivalence relation.

Exercise 3.5 gives some important information on how conjugacy relates to the structure of a group. We describe this relationship more fully in Proposition 3.11.

Proposition 3.11

Let G be a group.

(a) The relation $\sim$ on elements of G defined by

$$a \sim b \text{ if, and only if, } a \text{ is conjugate to } b$$

is an equivalence relation.

(b) The conjugacy classes of G partition the group.

Proof

(a) This is shown in Exercise 3.5.

(b) This follows from part (a), since the equivalence classes of $\sim$ on G are precisely the conjugacy classes. We know that the equivalence classes of an equivalence relation on a set X form a partition of X. We can check this directly for $\sim$ on G as follows.

- Every element of G is conjugate to itself (by reflexivity of $\sim$) and so it belongs to a conjugacy class. Thus the union of the conjugacy classes is G.
- Suppose that an element $c \in G$ belongs to two conjugacy classes $\mathrm{Conj}_G(a)$ and $\mathrm{Conj}_G(b)$ for $a, b \in G$. Then $c \sim a$ and $c \sim b$. By symmetry of $\sim$, we have $a \sim c$, and so $a \sim b$ by transitivity. Thus all the elements of $\mathrm{Conj}_G(b)$ are conjugate to a and vice versa, so

  $$\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b).$$

  We have shown that two conjugacy classes either are the same or have empty intersection. ■

Exercise 3.6

Write down the conjugacy classes of S_3.

This exercise might have reminded you that two elements of the group S_n of permutations on n elements are conjugate if, and only if, they have the same cycle type. This is worth remembering when working with symmetric groups.

The conjugacy classes and the normal subgroups of a group G are in fact related, as the following proposition shows.

Proposition 3.12

Let G be a group.

(a) Any normal subgroup N of G is a union of conjugacy classes.

(b) Any subgroup H of G that is a union of conjugacy classes is a normal subgroup of G.

Proof

(a) We claim that N is the union of the conjugacy classes of its elements, namely

$$N = \bigcup_{a \in N} \mathrm{Conj}_G(a).$$

For any $a \in N$ we have $a \in \mathrm{Conj}_G(a)$, so $N \subseteq \bigcup_{a \in N} \mathrm{Conj}_G(a)$.

Now let $a \in N$, and consider any element gag^{-1} of $\mathrm{Conj}_G(a)$. By Proposition 3.7(a), we have $gag^{-1} \in N$. This shows that $\mathrm{Conj}_G(a) \subseteq N$ for any $a \in N$, hence $\bigcup_{a \in N} \mathrm{Conj}_G(a) \subseteq N$.

(b) Let $h \in H$. Since H is a union of conjugacy classes, there is $a \in G$ such that $h \in \mathrm{Conj}_G(a)$ and $\mathrm{Conj}_G(a) \subseteq H$. Then $h = kak^{-1}$ for some $k \in G$.

Now let $g \in G$. Then

$$ghg^{-1} = g(kak^{-1})g^{-1} = (gk)a(gk)^{-1} \in \mathrm{Conj}_G(a).$$

Since $\mathrm{Conj}_G(a) \subseteq H$, we have that $ghg^{-1} \in H$. Therefore $gHg^{-1} \subseteq H$ for all $g \in G$. By Proposition 3.7(a), H is a normal subgroup of G. ■

3.2 Quotient groups

From the previous section we know that the cosets of a subgroup H of a group G form a partition of G. When H is a normal subgroup, we can say more: we may define a binary operation on the set of cosets of H that makes the set of cosets into a group.

From here on in this module, when we refer to a coset of a subgroup we mean a *left* coset, unless otherwise specified.

The set of left cosets of a normal subgroup N in G is denoted by G/N. The symbol G/N is read either as 'the quotient of G by N' or, for reasons we will explain shortly, as 'G mod N'.

The binary operation that makes G/N into a group is defined as follows.

Definition 3.13 *Product of cosets*

Let G be a group, N be a normal subgroup of G and let $a, b \in G$. We define the **product** of the cosets aN and bN to be

$$(aN)(bN) = (ab)N.$$

Our definition ensures that the product of two cosets of N is a coset of N. But is this coset unique, that is, is the product of cosets a *well-defined* operation? For example, as we have already seen, it is quite possible for $aN = a_1N$ and $bN = b_1N$ for some elements a_1 and b_1 different from a and b. If this is the case, the product $(aN)(bN) = (a_1N)(b_1N)$ has been defined to be both $(ab)N$ and $(a_1b_1)N$. So our definition will produce a well-defined binary operation only if each such product is uniquely defined, that is, if $(ab)N = (a_1b_1)N$.

The following theorem proves that the product in Definition 3.13 is well defined.

Theorem 3.14

Let G be a group, N be a normal subgroup of G and a, a_1, b and b_1 be elements of G such that

$$aN = a_1N \quad \text{and} \quad bN = b_1N.$$

Then

$$(ab)N = (a_1b_1)N.$$

Proof By Proposition 2.11, to show that $(ab)N = (a_1b_1)N$ it is enough to show that $(ab)^{-1}(a_1b_1)$ is in N.

Now, $(ab)^{-1}a_1b_1 = b^{-1}a^{-1}a_1b_1$.

Since $aN = a_1N$, Proposition 2.11 tells us that $a^{-1}a_1 \in N$, and therefore $b^{-1}a^{-1}a_1 \in b^{-1}N$.

But N is normal, so $b^{-1}N = Nb^{-1}$ and therefore $b^{-1}a^{-1}a_1 = nb^{-1}$, for some n in N. So $(ab)^{-1}a_1b_1 = nb^{-1}b_1$ with n in N.

But Proposition 2.11 also tells us that $b^{-1}b_1 \in N$, and so $(ab)^{-1}a_1b_1$ is a product of two elements of N, namely n and $b^{-1}b_1$. Since N is a group, it follows that $(ab)^{-1}a_1b_1 \in N$. ■

Theorem 3.14 is the first step in proving that the set of cosets G/N, with binary operation defined by $(aN)(bN) = (ab)N$, is a group. In future we will often write $aNbN$ instead of $(aN)(bN)$, and abN instead of $(ab)N$.

All we now need to do is check that the group axioms are satisfied.

The closure axiom is satisfied since, as we remarked above, $(ab)N \in G/N$.

Exercise 3.7

(a) Check that the binary operation we have defined on the set of cosets G/N is associative.

(b) Prove that the coset N $(= eN)$ is the identity of G/N.

(c) Prove that the inverse of the coset aN in G/N is $a^{-1}N$.

The results in Theorem 3.14 and Exercise 3.7 enable us to give the following definition.

Definition 3.15 *Quotient group*

Let N be a normal subgroup of the group G. The **quotient group of G with respect to N** is defined as the group whose underlying set is G/N and whose operation is given by

$$(aN)(bN) = (ab)N \text{ for any } aN, bN \in G/N.$$

Since aN and bN are both subsets of G, we could have defined their product $(aN)(bN)$ as the product of subsets; that is,

$$(aN)(bN) = \{xy : \ x \in aN, \ y \in bN\}.$$

This definition has the advantage that the product is well defined, since it depends on the cosets as a whole rather than on the particular elements a and b in the cosets. On the other hand, with this definition it is not immediately clear whether or not the product of two cosets is itself a coset of N. In fact, this definition *does* produce the same product as Definition 3.13, as you will find out in the following exercise.

Exercise 3.8

Prove that if N is a normal subgroup of a group G then

$$\{xy : \ x \in aN, \ y \in bN\} = \{(ab)n : \ n \in N\}.$$

Since $\{(ab)n : \ n \in N\} = (ab)N$, Exercise 3.8 does indeed show that the two products of cosets defined in this subsection are in fact the same.

In the following exercise you can find out what happens when you attempt to multiply two cosets of a subgroup that is not normal.

Exercise 3.9

Let $G = S_3$ be the group of permutations on three elements and let $H = \{e, (1\,2)\}$.

(a) Write down the left cosets of H.

(b) Show that multiplication of these cosets, as described in Definition 3.13, is not well defined.

In the following discussion we consider a quotient group G/H of an abelian group G. In additive notation, the left coset of H containing $a \in G$ is written

$$a + H.$$

We will now illustrate the construction of a quotient group of the abelian group $(\mathbb{Z}, +)$. Consider the set

$$N = 4\mathbb{Z} = \{4z : \ z \in \mathbb{Z}\}.$$

First, N is a subgroup of $(\mathbb{Z}, +)$. The proof is straightforward and is virtually the same as for $2\mathbb{Z}$, which we discussed in Section 2.

Next, since $(\mathbb{Z}, +)$ is abelian, N is normal by Exercise 3.2.

Let us now determine the distinct cosets of N, i.e. the elements of $\mathbb{Z}/N = \mathbb{Z}/4\mathbb{Z}$.

By Proposition 2.11, the cosets $a + N$ and $b + N$ are equal if, and only if, $a + (-b) \in N$ – in other words if, and only if, a and b differ by a multiple of 4. Thus, two elements of $\mathbb{Z}$ are in the same coset if, and only if, they are equal modulo 4.

Therefore, in additive notation the distinct cosets are

$$\begin{aligned}
0 + 4\mathbb{Z} &= \{4z : \ z \in \mathbb{Z}\} = 4\mathbb{Z}, \\
1 + 4\mathbb{Z} &= \{1 + 4z : \ z \in \mathbb{Z}\}, \\
2 + 4\mathbb{Z} &= \{2 + 4z : \ z \in \mathbb{Z}\}, \\
3 + 4\mathbb{Z} &= \{3 + 4z : \ z \in \mathbb{Z}\}.
\end{aligned}$$

It is clear that the sum of the cosets $a + N$ and $b + N$ is determined by the sum of a and b modulo 4.

The language here is often carried over to the general case. This is why the quotient group G/N is often referred to as 'G mod N'. Calculations in the quotient group G/N are like those in G, except that the elements of N are treated as if they were the identity. Thus the quotient group is, in some sense, the group we obtain from the group G by regarding each element $n \in N$ as the identity. We will say more about this aspect of quotient groups later in the chapter.

Exercise 3.10

Let $G = S_3$ be the group of permutations on three elements.

(a) Write down the only proper non-trivial normal subgroup N of S_3.

(b) Write out the Cayley table of G/N.

4 Isomorphisms and homomorphisms

This section gives a mathematical definition of the idea that two groups can have the same structure – that is, that they can be isomorphic. It also explores the more general notion of a homomorphism between two groups (that is, a map that preserves the group operation) and the consequences of the existence of such a map: the First Isomorphism Theorem and the Correspondence Theorem.

4.1 Isomorphisms

In this subsection our aim is to determine under what conditions two groups with the same number of elements are 'essentially the same' group. The first problem to be solved in answering this question is to define formally what we mean by saying that two groups are 'essentially the same'. We will define two groups to be 'essentially the same' if they are *isomorphic*, a concept that you are likely to have met in your previous mathematical studies. However, we delay the formal definition until we have looked at some examples in detail.

As an example of a group having four elements, consider an abstract group $\{e, a, b, c\}$ with the following Cayley table.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group is called the **Klein group**, and often denoted by V.

We have already seen other examples of groups with four elements. First, in Subsection 1.3, we met $\Gamma(\square)$, the group of symmetries of the rectangle, with the following Cayley table.

$\circ$	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

Then, in Example 1.9, we met the group of non-zero integers with multiplication modulo 5, whose underlying set is $\{1, 2, 3, 4\}$. Here we will denote this group by $(\mathbb{Z}_5^*, \times_5)$; its Cayley table is as follows.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

In Subsection 1.5 we also met the groups $(\mathbb{Z}_n, +_n)$ of integers modulo n, with underlying set $\{0, 1, \ldots, n-1\}$ and addition modulo n for all positive integers n. The special case $n = 4$ gives another group with four elements.

Exercise 4.1

Write out the Cayley table for the group $(\mathbb{Z}_4, +_4)$.

The following exercise asks you to work with D_4, the group of symmetries of the square.

Exercise 4.2

Consider the subgroup R of the dihedral group D_4 generated by the rotation r about the centre O through an angle of $\frac{\pi}{2}$ anticlockwise. Prove that R has four elements, and write down its Cayley table.

Let us consider our initial question of whether any of these groups of four elements are 'essentially the same'. The five groups $(V, \circ)$, $(\Gamma(\square), \circ)$, $(\mathbb{Z}_5^*, \times_5)$, $(\mathbb{Z}_4, +_4)$ and $(R, \circ)$ are not identical, since the underlying sets are different and each has a different binary operation. However, the first two, $(V, \circ)$ and $(\Gamma(\square), \circ)$, are essentially the same in that their Cayley tables have the same pattern: the Cayley table for $(V, \circ)$ becomes the Cayley table for $(\Gamma(\square), \circ)$ by replacing a with r, b with h and c with v. Similarly, the Cayley tables of the fourth and fifth groups have the same pattern as one another, as shown below.

$(\mathbb{Z}_4, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(R, \circ)$

$\circ$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

The Cayley table for $(\mathbb{Z}_4, +_4)$ becomes the table for $(R, \circ)$ if we replace $+_4$ with $\circ$, 0 with e, 1 with r, 2 with r^2 and 3 with r^3.

These replacements in the headings of the Cayley tables define two bijections:

$$\psi : V = \{e, a, b, c\} \to \Gamma(\square) = \{e, r, h, v\}, \text{ and}$$
$$\phi : \mathbb{Z}_4 = \{0, 1, 2, 3\} \to R = \{e, r, r^2, r^3\}.$$

ψ is the Greek letter 'psi'.

In each case, applying the relevant bijection to the body of the first table produces the second table. This means that ψ and ϕ preserve the effect of the binary operations: the image of the combination of elements in the first table in each case is the same as the combination of their images in the second table. For example, in the second case, for all x and y in $\mathbb{Z}_4$ we have

$$\phi(x +_4 y) = \phi(x) \circ \phi(y).$$

This is what we mean when we say that two groups are 'essentially the same'. When this is the case, the groups are said to be *isomorphic*.

Definition 4.1 *Isomorphism of groups*

The groups $(G, \circ)$ and $(H, *)$ are **isomorphic** if, and only if, there exists a bijection $\phi : G \to H$ such that, for all a and b in G, we have

$$\phi(a \circ b) = \phi(a) * \phi(b).$$

Such a bijection is called an **isomorphism** from G to H.

We use the notation $G \cong H$ to denote that G is isomorphic to H.

In multiplicative notation for both groups, the condition in Definition 4.1 becomes

$$\phi(ab) = \phi(a)\phi(b).$$

This is the notation we will use most of the time. Where the binary operation in each group is addition, the corresponding statement is

$$\phi(a + b) = \phi(a) + \phi(b).$$

Exercise 4.3

Prove that the function $\phi : \mathbb{Z} \to 2\mathbb{Z}$ defined by

$$\phi : n \mapsto 2n$$

defines an isomorphism from $(\mathbb{Z}, +)$ to $(2\mathbb{Z}, +)$.

We proved that $(2\mathbb{Z}, +)$ was a group in Section 2.

In Definition 4.1, we stated the condition 'G and H are isomorphic' in terms of ϕ as 'ϕ is an isomorphism from G to H'. While the first condition is symmetric in G and H, the second is not. However, there is no conflict here, as the following proposition shows.

Proposition 4.2

Let G and H be groups and let ϕ be an isomorphism from G to H. Then ϕ^{-1} is an isomorphism from H to G.

Proof Since ϕ is a bijection, its inverse ϕ^{-1} is a bijection from H to G.

We need to prove that for any two elements x and y of the group H, we have

$$\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y).$$

Since the function ϕ is onto, there exist elements a and b in G such that $\phi(a) = x$ and $\phi(b) = y$ or, to put it another way, $a = \phi^{-1}(x)$ and $b = \phi^{-1}(y)$. Moreover, since ϕ is an isomorphism we have $\phi(ab) = \phi(a)\phi(b)$.

Therefore

$$\phi^{-1}(xy) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(x)\phi^{-1}(y). \quad \blacksquare$$

Back to our five example groups: so far we have shown that $(V, \circ)$ and $(\Gamma(\square), \circ)$ are isomorphic and that $(\mathbb{Z}_4, +_4)$ and $(R, \circ)$ are isomorphic. Are there any other isomorphisms among the five groups?

We have already seen that $(\mathbb{Z}_5^*, \times_5)$ and $(\mathbb{Z}_4, +_4)$ are both cyclic groups with four elements, so presumably they too are isomorphic. Their Cayley tables, however, do not seem to have the same pattern as one another.

$(\mathbb{Z}_4, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_5^*, \times_5)$

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

However, this might just mean that in assuming the elements of $\mathbb{Z}_4$ should correspond to the elements of $\mathbb{Z}_5^*$ in the same order as they appear in the headings of the tables, we are considering the wrong function ϕ. So far we have no clue as to how to look for a bijection from the underlying set of $\mathbb{Z}_4$ to that of $\mathbb{Z}_5^*$ that might show the Cayley tables have the same pattern. On the other hand, we have said that two isomorphic groups are 'essentially the same', so it should follow that corresponding elements will have the same properties. This is helpful when looking for a suitable bijection: for example, we would expect the identity of one group to correspond to the identity of the other. This is in fact the case.

Theorem 4.3

Let G and H be groups, let e be the identity of G and let ϕ be an isomorphism from G to H. Then $\phi(e)$ is the identity of H.

Proof As e is the identity for the group G, we know that $ea = a$ for any element a in G.

But ϕ is an isomorphism, so this gives $\phi(e)\phi(a) = \phi(a)$. Therefore $\phi(e)$ behaves like a left identity for the element $\phi(a)$ of H, and so it is the identity of H by Proposition 1.4 of this chapter. ■

By the same token, we expect the image of the inverse of an element under an isomorphism to correspond to the inverse of the image.

Exercise 4.4

Let G and H be groups, and let ϕ be an isomorphism from G to H. Let a be an element of G with inverse a^{-1}. Show that the inverse of $\phi(a)$ is $\phi(a^{-1})$, that is,

$$(\phi(a))^{-1} = \phi\big(a^{-1}\big).$$

Hint: as in the proof of Proposition 1.4, use one of the results from Section 1.

So now we know that if there is an isomorphism ϕ from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$, then the identity in $\mathbb{Z}_4$ must correspond to the identity in $\mathbb{Z}_5^*$, that is $\phi(0) = 1$, and that inverses must correspond to inverses.

In Example 1.9 we showed that $(\mathbb{Z}_5^*, \times_5)$ is a cyclic group by verifying that the element 2 is a generator. If there is an isomorphism ϕ from $(\mathbb{Z}_4, +_4)$ to this group, then surely a generator in one group must correspond to a generator in the other. So we might try letting the generator 1 in $\mathbb{Z}_4$ correspond to the generator 2 in $\mathbb{Z}_5^*$. Since 3 is the inverse of 1 in $\mathbb{Z}_4$ and 3 is the inverse of 2 in $\mathbb{Z}_5^*$, we should have $\phi(3) = 3$. Then ϕ must send 2 in $\mathbb{Z}_4$ to 4 in $\mathbb{Z}_5^*$.

In fact, when we write the Cayley table of $(\mathbb{Z}_5^*, \times_5)$ as

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

we find that it does have the same pattern as the Cayley table for $(\mathbb{Z}_4, +_4)$.

So the function $\phi : \mathbb{Z}_4 \to \mathbb{Z}_5^*$ defined by

$$\phi(0) = 1,\ \phi(1) = 2,\ \phi(2) = 4,\ \phi(3) = 3$$

is an isomorphism from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

Exercise 4.5

Find another isomorphism from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

We have seen that $(\mathbb{Z}_4, +_4)$ is isomorphic to $(R, \circ)$ and to $(\mathbb{Z}_5^*, \times_5)$, and we can deduce that $(R, \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ are isomorphic. We have also seen that $(V, \circ)$ and $(\Gamma(\square), \circ)$ are isomorphic. But is there an isomorphism between $(\mathbb{Z}_4, +_4)$ and $(\Gamma(\square), \circ)$, say, in which case we could deduce that all five groups are isomorphic? The answer is no, but how do we go about showing this?

This would follow because the inverse of an isomorphism is an isomorphism, as is the composite of two isomorphisms.

In order to determine whether or not $(\Gamma(\square), \circ)$ is isomorphic to $(\mathbb{Z}_4, +_4)$, we might think we need to consider all possible ways of writing out its Cayley table, and see whether any of the rearrangements has the same pattern as our table for $(\mathbb{Z}_4, +_4)$. Equivalently, we would have to consider all the bijections from $\mathbb{Z}_4$ to $\Gamma(\square)$ and check whether any of these satisfies the isomorphism property.

At first glance this seems to mean checking $4! = 24$ tables, since that is the number of ways of rearranging four elements. We already know that identity elements must correspond and so must inverses, which cuts down the work somewhat. Nevertheless, this method still involves a considerable amount of effort.

For larger groups this approach would be even more laborious, and it is not a practical way to prove or disprove the existence of an isomorphism between large finite groups. For infinite groups this approach is impossible, since there are an infinite number of possible bijections to consider.

Nevertheless, in practice it is often easier to prove that groups are *not* isomorphic than that they *are*. But why, you might well ask, might we want to know that two groups are not isomorphic?

Well, one of the main objectives of this part of the module is to classify certain classes of groups so that groups that are not isomorphic fall into different classes. In particular, we will classify finite abelian groups. That is, we will know what possible structures an abelian group of a given order can have.

Since isomorphic groups are 'essentially the same', they, and their corresponding elements, must have identical algebraic properties.

We use the word 'algebraic' here since it is possible for two groups to be isomorphic and yet to have different *geometric* properties. Consider, for example, the group of the symmetries of the rectangle (Subsection 1.3): the subgroup $\{e, r\}$ is isomorphic to the subgroup $\{e, h\}$ even though one contains a rotation and the other a reflection.

One way we can show that two groups are not isomorphic is to show that the groups have different algebraic properties.

One property of a finite group is its order, that is, the number of elements it has. Thus, one basic way in which two groups might be different is when they have different numbers of elements. In this case there is no bijection from one group to the other, and so the groups cannot be isomorphic. In particular, it is not possible for a finite and an infinite group to be isomorphic.

However, when two groups have the same number of elements we need to consider properties other than their order to show that they are not isomorphic.

Exercise 4.6

Let G and H be groups, and let ϕ be an isomorphism from G to H.

(a) Prove that if G is abelian, then so is H.

(b) Prove that the groups $\mathbb{Z}_6$ and S_3 are not isomorphic.

The solution to Exercise 4.6 provides one consequence of the existence of an isomorphism between two groups: if one of the groups is abelian, then so is the other. There is a corresponding negative result: an abelian group cannot be isomorphic to a non-abelian one.

Another useful property in deciding whether or not groups are isomorphic is the number of elements in the group having a given order. The definition of the *order of an element* is as follows.

Definition 4.4 *Order of a group element*

Let a be an element of a group G and let e be the identity in G. Then a has **order** n if, and only if, n is the smallest positive integer such that $a^n = e$. If no such positive integer exists, then the element a is said to have **infinite order**.

We use the notation $|a|$ to denote the order of an element a of finite order.

We have now used the word 'order' in two senses: in Section 2 we defined the order of a group and here we have defined the order of a group element. These two are consistent: one consequence of Definition 4.4 is that the order of an element is the order of the cyclic subgroup that it generates. If $a \in G$ has order n, then $|\langle a \rangle| = n$. Even the use of the modulus notation is shared.

Proposition 4.5

Let G be a finite group of order n and let $g \in G$. Then the order of g divides n.

Proof Since G is a finite group, g must have finite order, m say. Then g generates a cyclic subgroup $\langle g \rangle$ of G that has order m. By Lagrange's Theorem, m must divide n. ■

Exercise 4.7

Let G be a group and $g \in G$. Suppose that $g^n = e$ for some $n \in \mathbb{N}$. Show that the order of g is finite and that it divides n.

Hint: use the Division Algorithm (Book A, Chapter 1, Theorem 4.1) to write $n = qm + r$, where $m = |g|$ and $0 \leq r < m$.

Exercise 4.8

Let G be a group of order p where p is a prime. Show that G is cyclic.

Theorem 4.6

Let G and H be groups and let ϕ be an isomorphism from G to H. Then if $a \in G$ has finite order n, so does $\phi(a) \in H$.

Proof Let e be the identity of G, f be the identity of H and m be the order of $\phi(a)$. Since a has order n, we know that $a^n = e$ and so $\phi(a^n) = \phi(e)$. Now, using Theorem 4.3, we can say that

$$(\phi(a))^n = \phi(a^n) = \phi(e) = f.$$

Here we are using that $\phi(a^n) = (\phi(a))^n$. This is a straightforward extension of the property $\phi(ab) = \phi(a)\phi(b)$.

This tells us that $|\phi(a)| \leq |a|$, that is $m \leq n$, as the order of $\phi(a)$ is the *smallest* positive integer power of $\phi(a)$ that produces the identity f.

As $\phi(a)$ has order m, we know that $(\phi(a))^m = f$, so

$$\phi(a^m) = (\phi(a))^m = f = \phi(e).$$

However, ϕ is a one–one function, so this implies that $a^m = e$.

But a has order n and so $n \leq m$, by the minimality of n. Combining this with the fact that $m \leq n$ gives $m = n$, and so the order of a is the same as the order of $\phi(a)$. ■

Exercise 4.9

Let G and H be groups and let ϕ be an isomorphism from G to H. Prove that if the element a of G has infinite order, then so does $\phi(a)$.

Hint: use the fact that ϕ^{-1} is an isomorphism from H to G to show that if $\phi(a)$ has finite order, then so does a.

Finally, Theorem 4.6 enables us to say that the groups $\mathbb{Z}_4$ and $\Gamma(\square)$ are not isomorphic. The group $\mathbb{Z}_4$ has two elements of order 4 (1 and 3), whereas $\Gamma(\square)$ has no elements of order 4 (each of the non-identity elements has order 2). So having two elements of order 4 is a property that one group has and the other does not.

Alternatively, we could have shown that these two groups are not isomorphic by remarking that one of them is cyclic whereas the other is not. You might think that is an easier way to get our result, but in essence Theorem 4.6 is one way of showing that this is a correct argument, as the fact that $\mathbb{Z}_4$ has an element of order 4 is equivalent to the fact that it is a cyclic group, and the fact that $\Gamma(\square)$ has no element of order 4 shows that it is not cyclic. We will see, however, that Theorem 4.6 has a wider application than just to cyclic groups.

4.2 Homomorphisms

In Subsection 4.1 we saw that two groups $(G, \circ)$ and $(H, *)$ are isomorphic when there is a bijection $\phi : G \to H$ such that, for all a and b in G, we have $\phi(a \circ b) = \phi(a) * \phi(b)$.

If we do not require that ϕ should be one–one and onto, we still obtain a significant notion – that of *homomorphism*.

Definition 4.7 *Homomorphism*

Let $(G, \circ)$ and $(H, *)$ be groups. A function $\phi : G \to H$ is a **homomorphism** from G to H if, for all a and b in G, we have

$$\phi(a \circ b) = \phi(a) * \phi(b).$$

The property $\phi(a \circ b) = \phi(a) * \phi(b)$ is referred to as the **morphism** or **homomorphism property**.

So isomorphisms are also homomorphisms, but not all homomorphisms are isomorphisms, since a homomorphism is not necessarily one–one or onto.

Example 4.8 *A homomorphism that is neither one–one nor onto*

Consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_4, +_4)$ and the function ϕ from $\mathbb{Z}$ to $\mathbb{Z}_4$ defined by

$$\phi(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 2, & \text{if } n \text{ is odd.} \end{cases}$$

We can see that ϕ is neither one–one (since, for example, $\phi(0) = \phi(2) = 0$) nor onto (since, for example, 1 is not in the image set of ϕ).

We claim that ϕ is a homomorphism. To check this, we must check the morphism property – that is, that for all m and n in $\mathbb{Z}$,

$$\phi(m + n) = \phi(m) +_4 \phi(n).$$

Using the definition of ϕ, this can be done by considering four cases, determined by whether m and n are even or odd.

If m and n are both even, so is $m + n$ and therefore

$$\phi(m + n) = 0 = 0 +_4 0 = \phi(m) +_4 \phi(n).$$

If m is odd and n is even, then $m+n$ is odd and therefore

$$\phi(m+n) = 2 = 2 +_4 0 = \phi(m) +_4 \phi(n).$$

If m is even and n is odd, then $m+n$ is odd and therefore

$$\phi(m+n) = 2 = 0 +_4 2 = \phi(m) +_4 \phi(n).$$

If m and n are both odd, then $m+n$ is even and therefore

$$\phi(m+n) = 0 = 2 +_4 2 = \phi(m) +_4 \phi(n).$$

Therefore we have

$$\phi(m+n) = \phi(m) +_4 \phi(n) \text{ for all } m \text{ and } n \text{ in } \mathbb{Z}.$$

Hence ϕ is an example of a homomorphism that is neither one–one nor onto.

As you may recall from your previous mathematical studies, the set of elements that are mapped by a homomorphism to the identity in the codomain is called the *kernel* of the homomorphism.

Definition 4.9 *Kernel*

Let $\phi : G \to H$ be a homomorphism and let e be the identity in H. Then the **kernel** of ϕ is the set

$$\mathrm{Ker}(\phi) = \{x \in G : \ \phi(x) = e\}.$$

In Example 4.8, the kernel of ϕ consists of all those elements of $\mathbb{Z}$ that map to 0, the identity of $\mathbb{Z}_4$. These are the even integers, that is,

$$\mathrm{Ker}(\phi) = 2\mathbb{Z}.$$

Note that $\mathrm{Ker}(\phi)$ is a subgroup of the domain of ϕ.

Definition 4.10 *Image*

Let $\phi : G \to H$ be a homomorphism. Then the **image** of ϕ is the set

$$\mathrm{Im}(\phi) = \{h \in H : \ h = \phi(x) \text{ for some } x \in G\}.$$

In the case of Example 4.8,

$$\mathrm{Im}(\phi) = \{0, 2\},$$

which is a subgroup of the codomain of ϕ.

Exercise 4.10

Consider the function $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by

$$\phi : n \mapsto 3n.$$

(a) Show that ϕ is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$, but it is not an isomorphism.

(b) Find the kernel of ϕ and show that it is a subgroup of the domain.

(c) Find the image of ϕ and show that it is a subgroup of the codomain.

The results of the previous exercise generalise, and we can say rather more about the kernel than just that it is a subgroup of the domain.

Theorem 4.11

Let $\phi : G \to H$ be a homomorphism from G to H. Then:

(a) The kernel of ϕ is a normal subgroup of G.

(b) The image of ϕ is a subgroup of H.

Proof We use multiplicative notation throughout and we denote the identities of G and H by e_G and e_H respectively.

(a) **Closure** If k and l are in $\mathrm{Ker}(\phi)$, then $\phi(k) = \phi(l) = e_H$. Therefore $\phi(kl) = \phi(k)\phi(l) = e_H e_H = e_H$, and so $kl \in \mathrm{Ker}(\phi)$.

Identity In Theorem 4.3 we showed that for any *isomorphism* ϕ from G to H, if e_G is the identity of G then $\phi(e_G)$ is the identity e_H of H. But the proof of Theorem 4.3 only made use of the morphism property in the definition of an isomorphism, and so the result in the theorem holds for homomorphisms too. Thus $e_G \in \mathrm{Ker}(\phi)$.

Inverses From Exercise 4.4 we know that for any *isomorphism* ϕ from G to H, and for any $x \in G$,

$$\phi(x^{-1}) = (\phi(x))^{-1}.$$

But the solution to Exercise 4.4 only made use of the morphism property in the definition of an isomorphism, and so the result in the exercise holds for homomorphisms too. Hence, if $k \in \mathrm{Ker}(\phi)$ then $\phi(k) = e_H$, so $\phi(k^{-1}) = e_H^{-1} = e_H$. Thus $k^{-1} \in \mathrm{Ker}(\phi)$.

Hence $\mathrm{Ker}(\phi)$ is a subgroup of the domain G.

Normality If $a \in G$ and $k \in \mathrm{Ker}(\phi)$, then

$$\begin{aligned}\phi\left(aka^{-1}\right) &= \phi(a)\phi(k)\phi(a^{-1}) \\ &= \phi(a)e_H\left(\phi(a)\right)^{-1} \\ &= \phi(a)\left(\phi(a)\right)^{-1} \\ &= e_H.\end{aligned}$$

Therefore $aKa^{-1} \subseteq \mathrm{Ker}(\phi)$ for all a in G. So $\mathrm{Ker}(\phi)$ is a normal subgroup of G.

(b) **Closure** Let g and h be in $\mathrm{Im}(\phi)$. Then there exist a and b in G such that $\phi(a) = g$ and $\phi(b) = h$. Now ab is in G and $\phi(ab) = \phi(a)\phi(b) = gh$, showing that $gh \in \mathrm{Im}(\phi)$.

Identity Since $\phi(e_G) = e_H$, the homomorphism version of Theorem 4.3 implies that $e_H \in \mathrm{Im}(\phi)$.

Inverses If $h \in \mathrm{Im}(\phi)$, then $h = \phi(g)$ for some $g \in G$. Now, by the homomorphism version of Exercise 4.4,

$$\phi(g^{-1}) = (\phi(g))^{-1} = h^{-1}.$$

Therefore, since $g^{-1} \in G$, we have that $h^{-1} \in \mathrm{Im}(\phi)$. ■

In the next exercise you will discover some group properties that are preserved by homomorphisms.

Exercise 4.11

Let G and H be groups and let $\phi : G \to H$ be a homomorphism.

(a) Show that if G is abelian, then so is $\phi(G)$, the image of G under ϕ.

(b) Let g be an element of finite order n in G. Show that $\phi(g)$ has finite order m, where m divides n.

Theorem 4.11 tells us that a homomorphism ϕ from G to H gives rise to a normal subgroup $\mathrm{Ker}(\phi)$ of the domain G. This normal subgroup can be used to define the quotient group $G/\mathrm{Ker}(\phi)$.

We have also seen that ϕ gives rise to a subgroup of the codomain H, namely $\mathrm{Im}(\phi)$.

It turns out that the quotient $G/\mathrm{Ker}(\phi)$ and the image $\mathrm{Im}(\phi)$ are isomorphic. Before giving a proof of this result, we illustrate it by expanding an example considered earlier.

Example 4.12 *An isomorphism between* $\mathbb{Z}/2\mathbb{Z}$ *and* $(\{0, 2\}, +_4)$

Let ϕ be the homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_4$ defined in Example 4.8 by

$$\phi(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 2, & \text{if } n \text{ is odd.} \end{cases}$$

In the discussion following Definition 4.9, we found that $\mathrm{Ker}(\phi) = 2\mathbb{Z}$ and $\mathrm{Im}\,\phi = \{0, 2\}$.

The cosets of $\mathrm{Ker}(\phi) = 2\mathbb{Z}$ are

$0 + \mathrm{Ker}(\phi) = 2\mathbb{Z}$, the set of even integers, and
$1 + \mathrm{Ker}(\phi) = 1 + 2\mathbb{Z}$, the set of odd integers.

Since both $\mathbb{Z}/\operatorname{Ker}(\phi)$ and $\operatorname{Im}(\phi)$ are cyclic groups of order 2, they are isomorphic. Because isomorphisms take identities to identities, the only possible isomorphism $\psi : \mathbb{Z}/\operatorname{Ker}(\phi) \to \operatorname{Im}(\phi)$ is given by

$$\begin{cases} \psi(0 + \operatorname{Ker}(\phi)) = 0 = \phi(0), \\ \psi(1 + \operatorname{Ker}(\phi)) = 2 = \phi(1). \end{cases}$$

Thus $\psi(x + \operatorname{Ker}(\phi)) = \phi(x)$ for all $x \in \mathbb{Z}$.

It turns out that the definition of the isomorphism $\psi : \mathbb{Z}/\operatorname{Ker}(\phi) \to \operatorname{Im}(\phi)$ in Example 4.12 can be extended to the general case.

Theorem 4.13 *First Isomorphism Theorem*

Let $\phi : G \to H$ be a homomorphism from the group G to the group H, with kernel K and image I.

Then the function $\psi : G/K \to I$ defined by

$$\psi : gK \mapsto \phi(g)$$

is an isomorphism.

Proof Firstly, since ψ is defined in terms of a representative g of the coset gK rather than in terms of gK itself, we must check that ψ is well defined.

For this, we need to show that for any two elements a and b in G, if $aK = bK$ then $\psi(aK) = \psi(bK)$, that is $\phi(a) = \phi(b)$.

Suppose $aK = bK$. Then $a^{-1}b \in K$ by Proposition 2.11. Since K is the kernel of ϕ, this implies that $\phi\left(a^{-1}b\right) = e_H$, where e_H is the identity of H. So $\phi\left(a^{-1}\right)\phi(b) = (\phi(a))^{-1}\phi(b) = e_H$. Multiplying both sides by $\phi(a)$ on the left gives $\phi(a) = \phi(b)$, as required.

We use the homomorphism version of Exercise 4.4.

Secondly, we must show that ψ is one–one; that is, that $\psi(aK) = \psi(bK)$ implies $aK = bK$.

Now, by the way ψ is defined, the condition $\psi(aK) = \psi(bK)$ is equivalent to $\phi(a) = \phi(b)$. But if $\phi(a) = \phi(b)$, reversing the above argument gives $\phi\left(a^{-1}b\right) = e_H$. This means that $a^{-1}b \in K$, and so $aK = bK$ by Proposition 2.11.

Next, we must show that ψ is onto.

Any element h of I is of the form $\phi(a)$ for some element a of G. Then $h = \psi(aK)$, which shows that ψ is onto.

Lastly, we must show that ψ has the morphism property; that is, we need to check that $\psi(aK\,bK) = \psi(aK)\psi(bK)$ for all a and b in G. We have

$$\psi(aK\,bK) = \psi(abK) = \phi(ab) = \phi(a)\phi(b) = \psi(aK)\psi(bK).$$

This concludes the proof of the theorem. ■

Corollary 4.14

Suppose that $\phi : G \to H$ is a homomorphism from G to H such that

$$\mathrm{Ker}(\phi) = \{e\}.$$

Then ϕ is an isomorphism from G to $\phi(G) = \mathrm{Im}(\phi)$.

Proof This is the First Isomorphism Theorem in the case where $\mathrm{Ker}(\phi) = \{e\}$. ■

Theorem 4.11 says that all kernels of group homomorphisms are normal subgroups of the domain. Our final result in this subsection shows that the converse is also true: every normal subgroup is the kernel of a suitably defined homomorphism. Thus a subgroup is normal if, and only if, it is the kernel of a homomorphism.

We know that when N is a normal subgroup of a group G, the quotient G/N is a group. This quotient will be the codomain for the homomorphism of which N is the kernel. There is a natural association of the elements of G with the cosets of N: each $a \in G$ is associated with the coset aN to which it belongs.

When we formalise these ideas, we obtain the following theorem.

Theorem 4.15

Let N be a normal subgroup of a group G. Then the function ϕ defined by

$$\phi(a) = aN$$

is a homomorphism from G onto the quotient group G/N.

Furthermore, the kernel of ϕ is N.

Proof We start by noting that ϕ is indeed a function from G to G/N by the way it is defined.

We check the morphism property. For any a and b in G, we have

$$\phi(ab) = abN = aNbN = \phi(a)\phi(b).$$

Thus ϕ is a homomorphism from G to G/N.

We now show that ϕ is onto G/N. Any element of G/N is a coset aN for some element a of G. But aN is the image of the element a under ϕ, because we defined $\phi(a) = aN$. Hence the function ϕ is onto.

Finally, we find the kernel of ϕ. The identity element of G/N is N, therefore a is an element of the kernel of ϕ if, and only if, $\phi(a) = N$. Since $\phi(a) = aN$, we have that $a \in \mathrm{Ker}(\phi)$ if, and only if, $aN = N$. But

Proposition 2.10 implies that $aN = N$ if, and only if, $a \in N$. Hence $\mathrm{Ker}(\phi) = N$. ■

The function ϕ in Theorem 4.15 appears so often in applications that it deserves a specific name.

Definition 4.16 *Natural homomorphism*

Let N be a normal subgroup of a group G. Then the homomorphism $\phi : G \to G/N$ defined by

$$\phi : a \mapsto aN$$

is called the **natural homomorphism** from G onto G/N.

Exercise 4.12

Show that a quotient group of an abelian group is abelian.

4.3 The Correspondence Theorem

In this subsection we describe the relationship between the subgroups of a group G and the subgroups of a quotient of G by a normal subgroup.

More specifically, we will prove that if G is a group and N is a normal subgroup of G, there is a one–one correspondence between the subgroups of G that contain N and the subgroups of the quotient group G/N, and this correspondence preserves normality. This result is known as the *Correspondence Theorem*.

Figure 4.1 illustrates the correspondence.

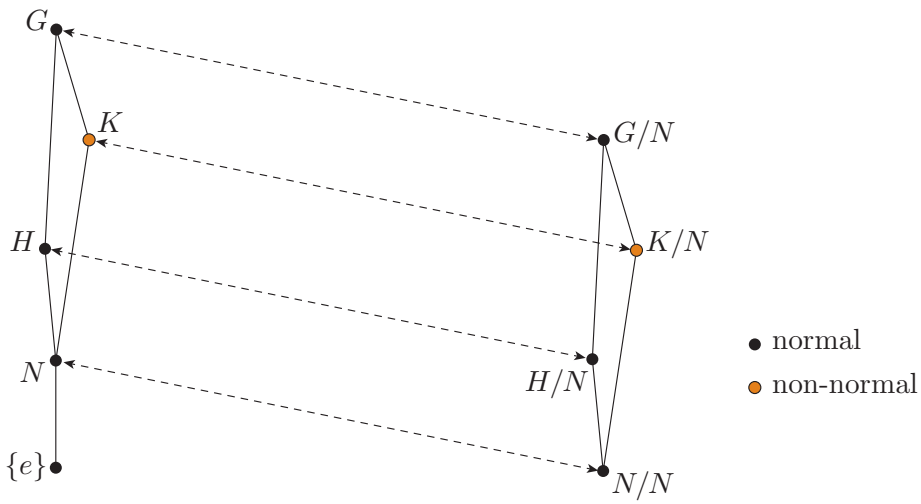


Figure 4.1 Correspondence Theorem

The correspondence can be described in more detail as follows: for any subgroup H of G that contains N, the corresponding subgroup in G/N is H/N. Moreover:

- if H is normal in G then H/N is normal in G/N
- if H is non-normal in G then H/N is non-normal in G/N.

Conversely, if $\overline{H}$ is a subgroup of G/N, then G has exactly one subgroup H that contains N and for which $\overline{H} = H/N$; this subgroup H is the subgroup of G corresponding to $\overline{H}$. Moreover:

- if $\overline{H}$ is normal in G/N then H is normal in G
- if $\overline{H}$ is non-normal in G/N then H is non-normal in G.

In particular, the Correspondence Theorem says that H is normal in G if, and only if, H/N is normal in G/N.

The result you are asked to prove in the following exercise shows you how to determine H from $\overline{H}$, and it will be used in the proof of the theorem.

Exercise 4.13

Observe that H is the set of elements of G that map to an element of $\overline{H}$ under the natural homomorphism.

Let $\overline{H}$ be a subgroup of G/N. Let H be the set defined by

$$H = \{h \in G : hN \in \overline{H}\}.$$

Prove that H is a subgroup of G containing N.

In fact, Exercise 4.13 shows you how to determine the subgroup H of G corresponding to a subgroup $\overline{H}$ of G/N. This will become clearer in the proof of the Correspondence Theorem, which we are now ready for.

Theorem 4.17 *Correspondence Theorem*

Let G be a group and let N be a normal subgroup of G. Then there is a one–one correspondence between the subgroups of G that contain N and the subgroups of the quotient group G/N. Moreover, this correspondence maps normal subgroups of G to normal subgroups of G/N and vice versa.

Proof Let G and N be as in the statement of the theorem.

α is the Greek letter 'alpha'.

Define a map α from the set of subgroups of G that contain N to the set of subgroups of the quotient group G/N by

$$\alpha(H) = \{hN : h \in H\} \text{ for any subgroup } H \text{ of } G \text{ containing } N.$$

The natural homomorphism ϕ and the map α have different domains and codomains: while ϕ maps elements of G to cosets of N in G, the map α takes subgroups of G to subgroups of G/N.

Observe that α is related to the natural homomorphism $\phi : G \to G/N$, in that $\alpha(H)$ is the image of the subgroup H under ϕ. Therefore, by Theorem 4.11 we have that $\alpha(H)$ is a subgroup of G/N. Moreover, from the way α has been defined, it preserves inclusions; that is, if $H \subseteq K$ then $\alpha(H) \subseteq \alpha(K)$.

Our aim is to show that α is one–one and onto and gives the required correspondence.

We start by showing that α is one–one. Suppose that H_1 and H_2 are two subgroups of G containing N such that

$$\alpha(H_1) = \alpha(H_2).$$

Let x_1 be an element of H_1. By the definition of α, the coset x_1N is an element of $\alpha(H_1) = \alpha(H_2)$. Hence there exists an element x_2 of H_2 such that $x_1N = x_2N$. Therefore, by the condition for the equality of cosets, $x_2^{-1}x_1 \in N$. Now, N is contained in H_2 and so

$$x_2^{-1}x_1 \in H_2.$$

But $x_2 \in H_2$ and so, by closure, $x_2(x_2^{-1}x_1) = x_1 \in H_2$. This shows that $H_1 \subseteq H_2$. All the conditions that we have used in this argument are symmetric in H_1 and H_2, so if we exchange the subscripts 1 and 2 throughout, we obtain a proof that $H_2 \subseteq H_1$. Hence $H_1 = H_2$ and α is one–one.

To show that α is onto, let $\overline{H}$ be a subgroup of G/N and define $H \subseteq G$ by

$$H = \{h \in G : \ hN \in \overline{H}\}.$$

Exercise 4.13 ensures that H is a subgroup of G containing N. We claim that $\alpha(H) = \overline{H}$.

Remember that

$$\alpha(H) = \{hN : \ h \in H\},$$

so from the definition of α we have that $h \in H$ if, and only if, $hN \in \overline{H}$. Hence $\alpha(H) = \overline{H}$, and α is onto.

We have established that α gives a one–one correspondence that is onto and preserves inclusion. We can also deduce from the definition of α that $\alpha(N) = \{N\}$, the trivial subgroup of G/N, and that $\alpha(G) = G/N$, the whole of the quotient group.

We now show that this correspondence sends normal subgroups to normal subgroups.

Firstly, assume that $H \leq G$ is a normal subgroup of G containing N and let $\overline{H} = \alpha(H)$. We want to show that $\overline{H}$ is normal in G/N. Let $x \in \overline{H}$ and $y \in G/N$. Then

$$x = hN \quad \text{for some } h \in H \text{ and}$$
$$y = gN \quad \text{for some } g \in G.$$

Since H is normal in G and $h \in H$, we have $ghg^{-1} \in H$.

Hence $yxy^{-1} = (gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = (ghg^{-1})N \in \overline{H}$.

This completes the proof that $\overline{H}$ is normal in G/N.

Now assume that $\alpha(H) = \overline{H}$ is a normal subgroup of G/N. Let $h \in H$ and $g \in G$. Then gN is an element of G/N and, by the correspondence, $hN \in \overline{H}$.

By the normality of $\overline{H}$,

$$(gN)(hN)(gN)^{-1} \in \overline{H}.$$

Hence $\overline{H}$ contains $(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = (ghg^{-1})N$.

Since $(ghg^{-1})N \in \overline{H}$, we have $ghg^{-1} \in H$. This completes the proof that H is normal in G. ■

Corollary 4.18

Let G be a group, N be a normal subgroup of G and H be a subgroup of G that contains N. If G is finite, the index of H in G is equal to the index of H/N in G/N; that is,

$$\frac{|G|}{|H|} = \frac{|G/N|}{|H/N|} = \frac{|\overline{G}|}{|\overline{H}|}.$$

The Correspondence Theorem can be used to investigate the structure of the subgroups of a given group: if N is a proper, non-trivial normal subgroup of a finite group G, then both G/N and N are smaller than G. More generally, G/N and N will be less complex than G, and so finding subgroups of G/N may be easier than finding subgroups of G. The Correspondence Theorem then gives the corresponding subgroups of G.

One consequence of the Correspondence Theorem is that every subgroup $\overline{H}$ of G/N has the form H/N for some $H \leq G$. Exercise 4.13 tells us how to find H from $\overline{H}$: remember that $H = \{h \in G : hN \in \overline{H}\}$, so in fact

$$H = \bigcup_{gN \in \overline{H}} gN,$$

the union of the cosets of N that belong to $\overline{H}$.

Since N is a normal subgroup of G, its left and right cosets are identical; we therefore refer simply to 'the cosets' of N in G.

The inclusion $H \subseteq \bigcup_{gN \in \overline{H}} gN$ follows from the definition of H. To see why the reverse inclusion holds, suppose that $h \in gN$ for some coset $gN \in \overline{H}$. Then $h = gn$ for some $n \in N$, so $hN = gnN = gN$ and therefore $h \in H$, as required.

Note also that when H is finite, the number of elements in H is the number of elements in N times the number of elements in $\overline{H}$; that is,

$$|\overline{H}| = \frac{|H|}{|N|} \quad \text{and} \quad |H| = |N| \times |\overline{H}|.$$

5 The group of permutations on four elements

In this section you will work through a series of exercises about the group S_4. This should consolidate the ideas covered in this chapter.

The first exercise is for you to practise cycle notation for permutations. Remember that we use e to denote the identity permutation.

Exercise 5.1

(a) Express the following products as products of disjoint cycles.

(i) $(1\,2\,3)(1\,2)$

(ii) $(1\,2\,3\,4)(1\,3)$

(iii) $(1\,3)(1\,2\,3\,4)$

(iv) $(1\,2)(1\,3\,4\,2)(1\,2)$

(v) $(1\,2\,3)(1\,4\,3\,2)(1\,4)$

(b) Write down the inverse of each of the permutations in part (a).

The next exercise asks you to check that certain sets of permutations are subgroups of S_4. Suppose you are asked to show that

$$H = \{e, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$$

is a subgroup of S_4. One way to establish closure is to compile the Cayley table of H, and then confirm that H contains the inverse of each of its elements. However, there are simpler methods. For instance, you might spot that H is the cyclic subgroup $\langle(1\,2\,3\,4)\rangle$ of S_4, so closure is immediate. Alternatively, the elements of H can be realised as the four rotational symmetries of a square whose corners are labelled 1, 2, 3 and 4: we know these symmetries form a group. Still another way is to look at the elements of H as the symmetry group of Figure 5.1.

You may remember from your previous studies the distinction between *direct* and *indirect* symmetries. For our purposes, the direct symmetries of a plane figure are the rotations, whereas the indirect symmetries are the reflections. The set of direct symmetries of any figure forms a group, as does the set of all symmetries.

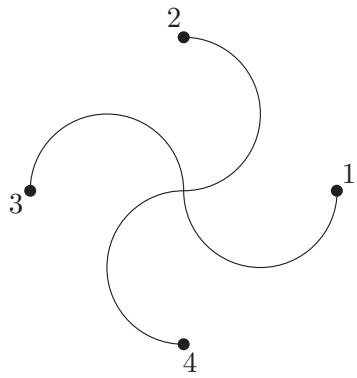


Figure 5.1 Figure whose symmetries give the subgroup $\langle(1\,2\,3\,4)\rangle$ of S_4

Thus, considering the symmetries of a plane figure gives a useful way to find subgroups of permutation groups (as shown in Figure 5.2 for S_4), as the following exercise illustrates.

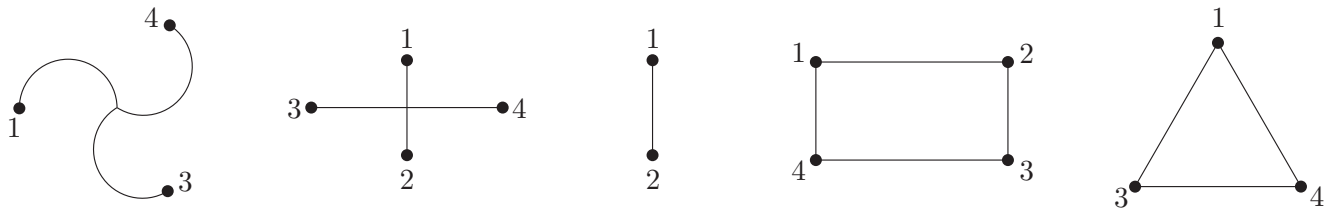


Figure 5.2 Figures whose symmetries give subgroups of S_4

Exercise 5.2

Show that each of the following subsets of S_4 is a group under composition of permutations.

(i) $H_1 = \{e, (1\,2)\}$

(ii) $H_2 = \{e, (1\,3\,4), (1\,4\,3)\}$

(iii) $H_3 = \{e, (1\,3), (1\,4), (3\,4), (1\,3\,4), (1\,4\,3)\}$

(iv) $H_4 = \{e, (1\,2), (3\,4), (1\,2)(3\,4)\}$

(v) $H_5 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

Hint: each of these sets can be related to one of the figures in Figure 5.2.

Another noteworthy example of a symmetry group is $\Gamma(\text{TET})$, the group of symmetries of a regular tetrahedron. This group contains 24 elements:

- the identity
- eight rotations about an axis through a vertex and the opposite face
- three rotations about a line joining opposite edges
- twelve other symmetries – six reflections in the plane through an edge joining two vertices and the midpoint of the edge joining the other two vertices, and six others, each obtained by composing a reflection and a rotation.

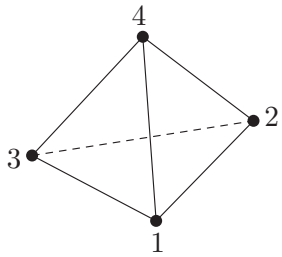


Figure 5.3 A tetrahedron with vertices 1, 2, 3 and 4

If we represent each symmetry by the way in which it permutes the vertices of the tetrahedron (labelled 1, 2, 3 and 4 as in Figure 5.3), we get precisely the elements of S_4. Thus, the groups $\Gamma(\text{TET})$ and S_4 are isomorphic.

Cosets are much maligned and misunderstood. In fact they often highlight interesting aspects of a group. It is often the case that a set H forms a subgroup of a group G because all the elements of H share a noteworthy property; moreover, the cosets of H partition G in such a way that all the elements in a single coset share a different but closely related property. Here is an example of what we mean.

Example 5.1 *Cosets in S_4*

We know from Exercise 5.2 that $H_3 = \{e, (1\,3), (1\,4), (3\,4), (1\,3\,4), (1\,4\,3)\}$ is a subgroup of S_4. Note also that $H_3 \cong S_3$. However, when H_3 is viewed as a subgroup of S_4, it is characterised by the property that each of its elements fixes 2.

When we consider the cosets of H_3 in S_4, we find that:

- every element of $(1\,2)H_3$ sends 2 to 1
- every element of $(2\,3)H_3$ sends 2 to 3
- every element of $(2\,4)H_3$ sends 2 to 4.

So the left cosets of H_3 partition S_4 in an interesting way.

The group H_3 in Example 5.1 is not normal in S_4, so the set of right cosets of H_3 in S_4 gives a different partition of S_4.

Exercise 5.3

Let H_3 be as in Exercise 5.2. For each right coset of H_3 in S_4, work out a property shared by its elements.

Viewing cosets in this way will be useful when you meet *group actions* in Chapter 6, as it will give interesting insights into the link between group actions and homomorphisms.

Now we begin a systematic search for *all* subgroups of S_4. First we use Lagrange's Theorem to find the possible orders of these subgroups. Then we look at the elements of S_4 and consider their cycle structure and order. Once we have done this, we will be in a position to find and list all the subgroups of S_4.

Recall that the alternating group A_n is a normal subgroup of S_n and consists of all the even permutations in S_n. In particular, A_4 has order 12.

Exercise 5.4

(a) What are the possible orders of the subgroups of S_4?

(b) The elements of S_4 have different cycle structures. For each of these cycle structures, write down one element, and the total number of elements with that structure. State the order of the elements of each type.

(c) Write down the orders of the elements of S_4, and how many elements there are of each order.

We now examine *conjugacy* in S_4: two elements g and h of S_4 are conjugate if there exists $k \in S_4$ such that $kgk^{-1} = h$.

We know that two permutations are conjugate in the symmetric group S_n if, and only if, they have the same cycle structure. So, for example, $(1\,2\,3)$ and $(1\,4\,2)$ are conjugate in S_4, as are $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$. However, the permutations $(1\,3)(2\,4)$ and $(1\,2)(2\,3)$ are not conjugate in S_4, since $(1\,2)(2\,3)$ is not the cycle form of a permutation, because it is not a product of *disjoint* cycles – in fact,

$$(1\,2)(2\,3) = (1\,2\,3).$$

Recall from Definition 3.9 of this chapter that the conjugacy class of an element g in a group G is the set of elements of G that are conjugate to g.

Exercise 5.5

(a) Calculate the conjugate hgh^{-1} of g in S_4, where

(i) $g = (1\,3)$, $h = (1\,2)(3\,4)$

(ii) $g = (1\,2\,3\,4)$, $h = (1\,4\,2)$.

(b) Find elements g_1 and g_2 in S_4 such that $g_1(1\,2)g_1^{-1} = (2\,4)$ and $g_2(1\,2\,3\,4)g_2^{-1} = (1\,3\,4\,2)$.

(c) How many conjugacy classes are there in S_4, and how many elements are there in each class?

The following exercise asks you to examine certain subgroups of S_4.

Exercise 5.6

(a) How many subgroups of order 2 does S_4 have, and how many of order 3?

(b) Find all cyclic subgroups of S_4 of order 4.

(c) The set $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a subgroup of S_4 called the *Klein subgroup*, as it is isomorphic to the Klein group, which you met in Subsection 4.1 of this chapter. Is V cyclic? Find all the subgroups of S_4 that are isomorphic to V.

(d) Why does S_4 not contain any *cyclic* subgroups of order 6?

(e) In Exercise 5.2 you showed that H_3 is a subgroup of S_4 of order 6. Find three further subgroups of S_4 of order 6.

(f) By considering the symmetry groups of various plane figures, find a subgroup of S_4 of order 8. Then find two more. Does S_4 contain any cyclic subgroups of order 8?

(g) Find a subgroup of S_4 of order 12.

Although we are not yet in a position to prove this, in Exercise 5.6 we found all the subgroups of S_4 of orders 2, 3, 4, 6, 8 and 12; that is, all the proper non-trivial subgroups.

Exercise 5.7

Describe in words the groups H_2 and H_3 of Exercise 5.2 and A_4 of Exercise 5.6 as subgroups of $\Gamma(\text{TET})$.

(It is rather more difficult, but interesting, to interpret all the other subgroups of S_4 in terms of the geometry of the tetrahedron.)

Recall from Definition 3.9 of this chapter that two subgroups H and K of G are said to be conjugate in G if there exists $g \in G$ such that $gHg^{-1} = K$.

Exercise 5.8

(a) Determine the subgroups $(1\,2)H_3(1\,2)^{-1}$ and $(1\,3\,2\,4)H_4(1\,3\,2\,4)^{-1}$, where H_3 and H_4 are as in Exercise 5.2.

(b) Are the subgroups H_4 and H_5 of Exercise 5.2 conjugate in S_4?

(c) Are all subgroups of order 2 conjugate to one another in S_4?

(d) Are all subgroups of order 3 conjugate to one another in S_4?

Exercise 5.9

Deduce from Proposition 3.12 and Exercise 5.4 that the only possible orders for non-trivial proper normal subgroups of S_4 are 4 and 12.

Confirm that normal subgroups of S_4 with orders 4 and 12 do indeed exist.

In Subsection 4.2 we saw that there is a correspondence between normal subgroups and kernels of group homomorphisms, in that the kernel of a homomorphism is a normal subgroup of the domain and, conversely, every normal subgroup of a group G is the kernel of some homomorphism with domain G.

Now you are asked to work with the important subgroup A_4 of S_4.

Exercise 5.10

(a) Recall that A_4 is a normal subgroup of S_4. If a homomorphism has domain S_4 and kernel A_4, how large is its image set?

(b) Write down a homomorphism whose domain is S_4 and whose kernel is A_4.

Hint: try a map with codomain $\mathbb{Z}_2$.

Exercise 5.11

(a) What are the possible orders of subgroups of A_4?

(b) Find all the subgroups of A_4 and give their orders. Does A_4 have a subgroup of order 6? What is the significance of this result?

(c) Are the elements $(1\,2\,3)$ and $(2\,3\,4)$ conjugate in A_4? (Careful!)

(d) Find the conjugacy classes in A_4 of elements of A_4.

(e) Find all non-trivial proper normal subgroups of A_4.

Exercise 5.12

Use your results from this section to complete the following table.

	S_4	A_4
(a) order of group		
(b) number of subgroups of order 2		
(c) number of subgroups of order 3		
(d) number of cyclic subgroups of order 4		
(e) number of non-cyclic subgroups of order 4		
(f) number of cyclic subgroups of order 6		
(g) number of non-cyclic subgroups of order 6		
(h) number of subgroups of order 8		
(i) number of subgroups of order 12		
(j) total number of subgroups		
(k) total number of normal subgroups		

Exercise 5.13

Show the relations given by the Correspondence Theorem between S_4, with its normal subgroups A_4 and V, and the quotient group S_4/V in a diagram similar to that in Figure 4.1.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Use the group axioms to check whether a given set with a specified binary operation is a group.

(b) Check whether a given subset of a group is a subgroup.

(c) Obtain the symmetry groups of simple geometric figures.

(d) Decide whether a group is cyclic.

(e) Partition a group into cosets of a given subgroup.

(f) Check whether a given subgroup of a group is normal.

(g) Form and identify quotient groups in simple cases.

(h) Check whether a given function between two groups is an isomorphism or a homomorphism.

(i) Decide whether two given groups are isomorphic.

(j) Find kernels and images of group homomorphisms.

(k) Compute products and conjugates of permutations.

(l) Construct proofs, similar to those in the chapter, based on the group axioms and the results of the chapter.

(m) Recognise familiar examples such as the Klein group, the cyclic groups $\mathbb{Z}_n$, the symmetry groups S_n and the alternating group A_4.

Solutions to exercises

Solution to Exercise 1.1

We need to check that the group axioms hold in each case. Since we are told we can assume associativity for matrix multiplication, we need only to check the other three axioms.

(a) **Closure** If $\mathbf{A}$ and $\mathbf{B}$ are two 2×2 matrices with real entries, the process of matrix multiplication guarantees that the product $\mathbf{AB}$ is 2×2 with real entries. This is not enough: we also need that the determinant of $\mathbf{AB}$ is non-zero. Recall that for any 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$,

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$$

(a proof of this result is reproduced below for completeness). Therefore if $\mathbf{A}$ and $\mathbf{B}$ both have non-zero determinants, so has $\mathbf{AB}$.

This completes the closure argument.

To see that $\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$, let

$$\mathbf{A} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad \text{and} \quad \mathbf{B} = \begin{bmatrix} e & g \\ f & h \end{bmatrix}.$$

Then $\mathbf{AB} = \begin{bmatrix} ae + cf & ag + ch \\ be + df & bg + dh \end{bmatrix}$ and so

$$\begin{aligned} \det(\mathbf{AB}) &= (ae + cf)(bg + dh) - (ag + ch)(be + df) \\ &= aebg + aedh + cfbg + cfdh - agbe - agdf - chbe - chdf \\ &= aedh + cfbg - agdf - chbe \\ &= ad(eh - gf) - bc(eh - gf) \\ &= (ad - bc)(eh - gf) \\ &= \det(\mathbf{A}) \det(\mathbf{B}). \end{aligned}$$

Identity The matrix $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ acts as an identity for matrix multiplication *and* has determinant 1, which is non-zero.

Inverses If $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\det(\mathbf{A}) = ad - bc \neq 0$, then

$$\mathbf{A}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Then $\mathbf{A}^{-1}$ has real entries. Moreover,

$$\det(\mathbf{A}) \det\left(\mathbf{A}^{-1}\right) = \det(\mathbf{A}\mathbf{A}^{-1}) = \det(\mathbf{I}) = 1,$$

so $\mathbf{A}^{-1}$ has non-zero determinant.

(b) **Closure** We take two typical elements and show that the product is of the right form to be in the specified set. So, suppose that a, b are in $\mathbb{Z}$. Then

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}.$$

Since $a + b$ is also in $\mathbb{Z}$, the product of the two matrices is also in the set. This proves closure.

Identity The matrix $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ acts as an identity for matrix multiplication. We need to check that it belongs to the set in question. Since the leading diagonal elements are 1, the bottom left element is 0 and the top right element is an integer (namely 0), $\mathbf{I}$ is in the set.

Inverses A typical element of the given set has the form $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and has determinant $1 \neq 0$, so it has a multiplicative inverse. We need to check that the inverse belongs to the specified set. We have

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix}.$$

Since $-a$ is an integer whenever a is, the inverse matrix has the required form and does indeed belong to the set.

Solution to Exercise 1.2

(a) We need to verify that $y^{-1}x^{-1}$ has the defining property of the inverse of xy, that is,

$$(xy)(y^{-1}x^{-1}) = e = (y^{-1}x^{-1})(xy).$$

Now

$$\begin{aligned} (xy)(y^{-1}x^{-1}) &= (x((yy^{-1})x^{-1})) && \text{(Associativity)} \\ &= x(ex^{-1}) && \text{(Identity)} \\ &= xx^{-1} && \text{(Identity)} \\ &= e, && \text{(Identity)} \end{aligned}$$

so $y^{-1}x^{-1}$ behaves as a *right* inverse for xy. Moreover,

$$\begin{aligned} (y^{-1}x^{-1})(xy) &= y^{-1}((x^{-1}x)y) && \text{(Associativity)} \\ &= y^{-1}(ey) && \text{(Identity)} \\ &= y^{-1}y && \text{(Identity)} \\ &= e. && \text{(Identity)} \end{aligned}$$

So $y^{-1}x^{-1}$ also behaves as a *left* inverse for xy.

Hence, by the uniqueness of inverses, $y^{-1}x^{-1}$ is the inverse of xy.

(b) We give a proof that uses the cancellation rules.

Because $\left(x^{-1}\right)^{-1}$ is the inverse of x^{-1}, we have

$$x^{-1}\left(x^{-1}\right)^{-1} = e.$$

On the other hand, x^{-1} is the inverse of x, and so $x^{-1}x = e$.

Equating the two expressions for e gives $x^{-1}\left(x^{-1}\right)^{-1} = x^{-1}x$, and left cancellation gives the desired result.

Solution to Exercise 1.3

(a) We are given that $gx = x$ and, by the identity axiom, we know that $ex = x$.

Hence $gx = ex$ and, by the right cancellation rule, $g = e$.

An alternative proof involves multiplying both sides of the equation $gx = x$ on the right by the element x^{-1}.

(b) We need to prove the following statement. Let G be a group with identity e and let x be an element of G. If g is an element of G such that $xg = x$, then $g = e$.

The proof is almost identical to that of part (a).

We are given that $xg = x$ and, by the identity axiom, we know that $xe = x$.

Hence $xg = xe$ and, by the left cancellation rule, $g = e$.

Solution to Exercise 1.4

We are given that $yx = e$ and, by the inverses axiom, we know that $x^{-1}x = e$. It follows that $yx = x^{-1}x\,(= e)$. Using the right cancellation rule, we have the required result that $y = x^{-1}$.

An alternative proof involves multiplying both sides of the equation $yx = e$ on the right by the element x^{-1}.

Solution to Exercise 1.5

(a) Since composition of functions is applied from right to left, the functions compose as follows:

$1 \mapsto 3 \mapsto 4$

$2 \mapsto 5 \mapsto 2$

$3 \mapsto 1 \mapsto 3$

$4 \mapsto 2 \mapsto 5$

$5 \mapsto 4 \mapsto 1.$

Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}.$$

(b) We start by tracing the image of 1, the image of this image, and so on, until we come back to 1. Then we consider the first number not already used and repeat the process. This gives

$$1 \mapsto 3 \mapsto 4 \mapsto 1$$
$$2 \mapsto 5 \mapsto 2.$$

Hence the original permutation can be written in cycle form as $(1\,3\,4)(2\,5)$.

Since the cycles in cycle form are disjoint, the order of the cycles does not matter. So $(1\,3\,4)(2\,5)$ and $(2\,5)(1\,3\,4)$ are equivalent cycle forms for this permutation.

(c) We start by tracing the image of 1, the image of the resulting number, and so on, until we come back to 1. Then we consider the first number not already used and repeat the process. As this is a product of cycles, we apply the cycles from right to left. We obtain the following.

$$1 \underbrace{\mapsto}_{(1\,3\,5\,6\,2)} 3 \underbrace{\mapsto}_{(2\,5\,4)} 3 \underbrace{\mapsto}_{(1\,6\,3)} 1$$

$$2 \underbrace{\mapsto}_{(1\,3\,5\,6\,2)} 1 \underbrace{\mapsto}_{(2\,5\,4)} 1 \underbrace{\mapsto}_{(1\,6\,3)} 6$$

$$6 \underbrace{\mapsto}_{(1\,3\,5\,6\,2)} 2 \underbrace{\mapsto}_{(2\,5\,4)} 5 \underbrace{\mapsto}_{(1\,6\,3)} 5$$

$$5 \underbrace{\mapsto}_{(1\,3\,5\,6\,2)} 6 \underbrace{\mapsto}_{(2\,5\,4)} 6 \underbrace{\mapsto}_{(1\,6\,3)} 3$$

$$3 \underbrace{\mapsto}_{(1\,3\,5\,6\,2)} 5 \underbrace{\mapsto}_{(2\,5\,4)} 4 \underbrace{\mapsto}_{(1\,6\,3)} 4$$

$$4 \underbrace{\mapsto}_{(1\,3\,5\,6\,2)} 4 \underbrace{\mapsto}_{(2\,5\,4)} 2 \underbrace{\mapsto}_{(1\,6\,3)} 2$$

Hence the product $(1\,6\,3)(2\,5\,4)(1\,3\,5\,6\,2)$ can be written in cycle form as $(1)(2\,6\,5\,3\,4)$, or more simply as $(2\,6\,5\,3\,4)$, since the absence of a symbol implies that it is fixed.

Note that you do not need to show the details of the calculations in your answer. We have included them here to show what should be done in your head, but the answer can normally be written down directly.

Solution to Exercise 1.6

(a) By the usual argument, corners must go to corners. Having moved one corner, there are only two places that an adjacent corner can be mapped to: the adjacent corners to the image corner. This gives a maximum of 12 symmetries.

There are six rotations about the centre O: through angles of 0, $\frac{\pi}{3}$, $\frac{2\pi}{3}$, $\frac{3\pi}{3}$ $(= \pi)$, $\frac{4\pi}{3}$ and $\frac{5\pi}{3}$ anticlockwise.

There are also six reflections: three in lines joining pairs of opposite corners, three in lines joining midpoints of opposite sides.

This shows that there are exactly 12 symmetries of a regular hexagon.

(b) Since r is rotation through $\frac{\pi}{3}$, r^6 will be rotation through $\frac{6\pi}{3} = 2\pi$ and so correspond to the identity. Now $r^6 = e$ means that $r^{-1} = r^5$. The result $sr = r^5 s$ now follows, since doing a rotation followed by a reflection is the equivalent of doing the reflection followed by the inverse of the rotation.

Solution to Exercise 1.7

Let G be a cyclic group generated by the element g. If x and y are any two elements of G, then for some integers m and n we have

$$x = g^m \quad \text{and} \quad y = g^n.$$

Then
$$\begin{aligned} xy &= g^m g^n \\ &= g^{m+n} && \text{(by the rule of indices)} \\ &= g^{n+m} && \text{(since addition in } \mathbb{Z} \text{ is commutative)} \\ &= g^n g^m && \text{(by the rule of indices)} \\ &= yx. \end{aligned}$$

Hence G is abelian.

Solution to Exercise 1.8

We consider the multiples modulo 6 of each element.

- The multiples of 1 are $1, 2, 3, 4, 5$ and 0, so 1 is a generator.
- The multiples of 2 are $2, 4$ and 0, so 2 does not generate the group.
- The multiples of 3 are 3 and 0, so 3 does not generate the group.
- The multiples of 4 are $4, 2$ and 0, so 4 does not generate the group.
- The multiples of 5 are $5, 4, 3, 2, 1$ and 0, so 5 is a generator (for example, $5 + 5 + 5 = 15 \equiv 3 \pmod 6$).

Solution to Exercise 1.9

From Example 1.9 we know that $4^2 \equiv 1 \pmod 5$. Therefore the only powers of 4 modulo 5 are 4 and 1, and so 4 is not a generator.

Solution to Exercise 2.1

Recall that $S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. We check that the conditions SG1, SG2 and SG3 hold for H.

The identity $e \in H$, so SG2 is satisfied.

As remarked, we need only check closure for pairs from $(1\,2\,3), (1\,3\,2)$. Since $(1\,2\,3)^2 = (1\,3\,2), (1\,3\,2)^2 = (1\,2\,3), (1\,2\,3)(1\,3\,2) = e$ and $(1\,3\,2)(1\,2\,3) = e$, condition SG1 is satisfied.

Finally, $(1\,2\,3)^{-1} = (1\,3\,2)$ and $(1\,3\,2)^{-1} = (1\,2\,3)$, so condition SG3 is satisfied.

Solution to Exercise 2.2

All subgroups must contain 0 (the identity), and any subgroup containing 1 or 5 is the whole group since both 1 and 5 are generators. The subgroups are as follows.

- The trivial subgroup $\{0\}$.
- The whole of $\mathbb{Z}_6$, that is, $\{0, 1, 2, 3, 4, 5\}$.
- $\{0, 2, 4\}$ – since 2 is in the group, $4 = 2 + 2 \pmod 6$ must be as well. If we include either 3 or 5, we necessarily include 1 (since $3 + 4 = 5 + 2 \equiv 1 \pmod 6$) and so we have the whole group.
- $\{0, 3\}$ – if we include either 2 or 4, we necessarily include 1 or 5 and so we have the whole group.

Solution to Exercise 2.3

We are given that H is a subgroup of the group G, so H satisfies the subgroup axioms. In particular, it is a subset of G.

Since it satisfies the identity axiom, H contains the identity element of G and so is non-empty. So H satisfies the first property.

Now suppose that x and y are any two elements of H. Since H satisfies the inverses axiom, and x is an element of H, we have that x^{-1} is an element of H. We now know that x^{-1} and y are elements of H. Being a subgroup, H satisfies the closure axiom, so the element $x^{-1}y$ is in H. So H satisfies the second property.

Solution to Exercise 2.4

For the 'if' part of the statement, we assume that H is a non-empty subset of G and that if x and y are in H then xy^{-1} is in H. We want to show that H is a subgroup of G, that is, that H satisfies the three subgroup axioms.

Identity By property (a), H is non-empty. Therefore there exists some element x in H. By property (b), if x and y are in H then xy^{-1} is in H. Taking $y = x$ shows that $xx^{-1} = e$ is in H.

Inverses If y is in H then, by the identity axiom (already verified), both e and y are in H. Property (b) then implies that $ey^{-1} = y^{-1}$ is in H.

Closure Let x and y be elements of H. By the inverses axiom (already verified), y^{-1} is an element of H. Therefore x and y^{-1} are both in H. So, by property (b), the product $x\left(y^{-1}\right)^{-1} = xy$ is in H.

For the 'only if' part, we assume that H is a subgroup of the group G, so it satisfies the subgroup axioms. In particular, H is a subset of G.

Since it satisfies the identity axiom, H contains the identity element of G and so is non-empty. So H satisfies property (a).

Now suppose that x and y are any two elements of H. Since H satisfies the inverses axiom, and y is an element of H, so is the element y^{-1}. We now know that x and y^{-1} are elements of H. Since H is a subgroup, it satisfies the closure axiom, so the element xy^{-1} is in H. So H satisfies property (b).

Solution to Exercise 2.5

(a) From the definition of a subgroup, the underlying set of K is a subset of the underlying set of H and hence of the underlying set of G. Furthermore K forms a group under the same group operation as H and hence, since H is a subgroup of G, under that of G. Thus K is a subgroup of G.

(b) This follows immediately from the definition since H and K both form groups under the same operation as G.

Solution to Exercise 2.6

We saw in Exercise 2.2 that the group $\mathbb{Z}_6$ under addition modulo 6 has subgroups $\{0, 3\}$ and $\{0, 2, 4\}$, and the union of these is $\{0, 2, 3, 4\}$.

This set is not a subgroup since it is not closed under addition modulo 6. For example, $2 + 3 \equiv 5 \pmod 6$ is not in the set.

An alternative reason why the set is not a subgroup is provided by a theorem due to Joseph-Louis Lagrange (1736–1813), which you will meet in Subsection 2.2, since the subset has four elements and 4 does not divide 6.

Solution to Exercise 2.7

Using additive notation, if H is a subgroup of the abelian group G then

$$x + y = y + x$$

for all $x, y \in G$ and, as H is a subset of G, certainly

$$x + y = y + x$$

for all $x, y \in H$.

Solution to Exercise 2.8

Recall that $S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. Then the cosets of $\{e, (1\,2)\}$ are as follows.

- $e\{e, (1\,2)\} = \{e, (1\,2)\}$
- $(1\,2)\{e, (1\,2)\} = \{(1\,2), (1\,2)(1\,2)\} = \{(1\,2), e\}$
- $(1\,3)\{e, (1\,2)\} = \{(1\,3), (1\,3)(1\,2)\} = \{(1\,3), (1\,2\,3)\}$
- $(2\,3)\{e, (1\,2)\} = \{(2\,3), (2\,3)(1\,2)\} = \{(2\,3), (1\,3\,2)\}$
- $(1\,2\,3)\{e, (1\,2)\} = \{(1\,2\,3), (1\,2\,3)(1\,2)\} = \{(1\,2\,3), (1\,3)\}$
- $(1\,3\,2)\{e, (1\,2)\} = \{(1\,3\,2), (1\,3\,2)(1\,2)\} = \{(1\,3\,2), (2\,3)\}$

Thus there are just three distinct left cosets, namely

$$\{e, (1\,2)\}, \quad \{(1\,3), (1\,2\,3)\} \quad \text{and} \quad \{(2\,3), (1\,3\,2)\}.$$

Solution to Exercise 2.9

We are given that $aH = bH$ and we must show that $a^{-1}b \in H$.

Since $b = be$, the element b is in the coset bH. But $aH = bH$, so $b \in aH$. Therefore there exists some $h \in H$ such that $b = ah$.

So $a^{-1}b = a^{-1}ah = h$, and therefore $a^{-1}b$ is in H.

Solution to Exercise 2.10

(a) To show that f is one–one, suppose that $f(x) = f(y)$. Then by the definition of f we have that

$$ax = ay.$$

Then $x = y$ by left cancellation. Hence f is one–one.

To show that f is onto, let z be any element in the codomain aH, so that $z = ah$ for some $h \in H$. Then by the definition of f we have $z = f(h)$. Hence f is onto.

(b) By part (a), the left cosets aH and bH each have the same number of elements as the subgroup H.

Solution to Exercise 2.11

Since $|S_3| = 6$, by Lagrange's Theorem we know that the possible sizes of subgroups of S_3 are 1, 2, 3 and 6. Here is a complete list:

- $\{e\}$, the trivial subgroup
- S_3, the whole group
- $\{e, (1\,2)\}$, a subgroup of order 2
- $\{e, (1\,3)\}$, a subgroup of order 2
- $\{e, (2\,3)\}$, a subgroup of order 2
- $\{e, (1\,2\,3), (1\,3\,2)\}$, a subgroup of order 3.

Solution to Exercise 2.12

By Proposition 2.6, $H \cap K$ is a subgroup of both H and K. By Lagrange's Theorem, the order of $H \cap K$ must divide both $|H|$ and $|K|$. But $|H|$ and $|K|$ are coprime, that is, their highest common factor is 1. This implies that $|H \cap K| = 1$ and so $H \cap K = \{e\}$.

Solution to Exercise 3.1

Since $\phi(aH)$ is defined in terms of a particular element a of the coset aH, and not in terms of aH itself, to show that ϕ is well defined we must show that if $aH = bH$ then $\phi(aH) = \phi(bH)$, that is, $Ha^{-1} = Hb^{-1}$.

Suppose that $aH = bH$. By Proposition 3.1, we have

$$Ha^{-1} = Hb^{-1} \quad \text{if, and only if,} \quad a^{-1}(b^{-1})^{-1} \in H.$$

But $a^{-1}(b^{-1})^{-1} = a^{-1}b$, and we know that $a^{-1}b \in H$ by our assumption that $aH = bH$ and Proposition 2.11. Therefore $Ha^{-1} = Hb^{-1}$, and so ϕ is well defined.

To show that ϕ is one–one, suppose that $\phi(aH) = \phi(bH)$, that is, $Ha^{-1} = Hb^{-1}$. From Proposition 3.1, we have that

$$a^{-1}(b^{-1})^{-1} = a^{-1}b \in H.$$

Therefore $aH = bH$ by Proposition 2.11, and so ϕ is one–one.

Finally, suppose that Hx is any right coset of H in G. Then $x^{-1} \in G$ and

$$\phi(x^{-1}H) = H\left(x^{-1}\right)^{-1} = Hx.$$

This shows that ϕ is onto.

Solution to Exercise 3.2

(a) We already know by Proposition 2.3 that both $\{e\}$ and G are subgroups of G.

If a is any element of G, then

$$a\{e\} = \{e\}a = \{a\}.$$

Hence $\{e\}$ is a normal subgroup of G.

To show that G is a normal subgroup of G, we show that if a is any element of G, then aG and Ga are both equal to G.

Since $a \in G$, Proposition 2.10 gives $aG = G$. By the corresponding result for right cosets, $Ga = G$. So for all $a \in G$, we have $aG = Ga = G$, and hence G is a normal subgroup of G.

(b) Suppose that H is a subgroup of the abelian group G and that $a \in G$.

The normality condition in additive notation is $a + H = H + a$ for all $a \in H$.

Any element of $a + H$ can be written as $a + h$ for some $h \in H$. Since G is abelian, $a + h = h + a$. This tells us that every element of $a + H$ is an element of $H + a$. Therefore

$$a + H \subseteq H + a.$$

Similarly,

$$H + a \subseteq a + H,$$

and equality follows. Hence H is a normal subgroup of G.

Solution to Exercise 3.3

(a) By Exercise 2.1, we know that H is a subgroup of G. By Exercise 2.10, H has two left cosets, namely H and $(1\,2)H = \{(1\,2), (1\,3), (2\,3)\}$. Similarly, H has two right cosets, namely H and $H(1\,2) = \{(1\,2), (1\,3), (2\,3)\}$. Since the left cosets of H are the same as the right cosets, H is a normal subgroup of G by Proposition 3.7(b).

(b) By the definition of index, H has exactly two left cosets and exactly two right cosets in G. One left (respectively right) coset of H is H itself.

From the proof of Lagrange's Theorem, we know that the left (respectively right) cosets of H in G form a partition of G. Therefore the other left (respectively right) coset is the difference $G \setminus H$. So the set of left cosets of H is the same as the set of right cosets, and the result follows by Proposition 3.7(b).

(c) Let N be the intersection of the given collection of normal subgroups of G. By Proposition 2.7, N is a subgroup of G.

Now suppose that H is any normal subgroup in the collection. Since $N \subseteq H$, by Proposition 3.7(a)

$$\begin{aligned} aNa^{-1} &\subseteq aHa^{-1} \\ &\subseteq H. \end{aligned}$$

This argument shows that aNa^{-1} is contained in *every* subgroup of the collection, and hence is contained in the intersection of the collection. That is,

$$aNa^{-1} \subseteq N,$$

and so N is a normal subgroup of G by Proposition 3.7(a).

Solution to Exercise 3.4

We use the subgroup criterion (Proposition 2.4).

To see that gHg^{-1} is not empty, note that $e \in H$ and so $geg^{-1} \in gHg^{-1}$.

Now let $x, y \in gHg^{-1}$. Then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. Thus

$$x^{-1}y = (gh_1g^{-1})^{-1}gh_2g^{-1} = gh_1^{-1}g^{-1}gh_2g^{-1} = g(h_1^{-1}h_2)g^{-1} \in gHg^{-1}.$$

Therefore gHg^{-1} is a subgroup of G.

Solution to Exercise 3.5

To show that $\sim$ is an equivalence relation, we need to show that it is reflexive, symmetric and transitive.

Since $a = eae^{-1}$ for all $a \in G$, any element a is conjugate to itself. This shows that $\sim$ is reflexive.

To see that $\sim$ is symmetric, suppose that $a \sim b$, so that $b = gag^{-1}$ for some $g \in G$. Then

$$g^{-1}bg = g^{-1}gag^{-1}g = eae = a,$$

hence $g^{-1}b(g^{-1})^{-1} = a$. Thus $b \sim a$.

For transitivity, suppose that $a \sim b$ and $b \sim c$. Then $b = gag^{-1}$ and $c = hbh^{-1}$ for some $g, h \in G$. Thus $c = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$, and so $a \sim c$.

Solution to Exercise 3.6

There are three conjugacy classes in S_3, namely

$$\{e\}; \{(1\,2), (1\,3), (2\,3)\}; \{(1\,2\,3), (1\,3\,2)\}.$$

Solution to Exercise 3.7

(a) Using the definition of the product of two cosets, and the associativity axiom for the group G, we have

$$\begin{aligned} aN(bNcN) &= aN(bcN) \\ &= a(bc)N \\ &= (ab)cN \\ &= (ab)NcN \\ &= (aNbN)cN. \end{aligned}$$

(b) As remarked, $N = eN$. So, for any element $aN \in G/N$, we have

$$NaN = eNaN = (ea)N = aN.$$

Similarly, $aNN = aN$. Hence N is the identity element of G/N.

(c) By the definition of the product in G/N,

$$a^{-1}NaN = (a^{-1}a)N = eN = N.$$

Similarly,

$$aNa^{-1}N = (aa^{-1})N = eN = N.$$

Hence $a^{-1}N$ is the inverse of aN.

Solution to Exercise 3.8

As usual, we need to prove two set inclusions. For convenience, let

$$P = \{xy : \ x \in aN, \ y \in bN\} \quad \text{and} \quad Q = \{(ab)n : \ n \in N\}.$$

Firstly we show that $P \subseteq Q$. Let z be an element of P. Then $z = an_1bn_2$ for some n_1 and n_2 in N. Now n_1b is an element of Nb. Since N is a normal subgroup, we know that $Nb = bN$, so $n_1b = bn_3$ for some n_3 in N. Therefore $z = an_1bn_2 = abn_3n_2$, which is an element of Q. This shows that $P \subseteq Q$.

To show that $Q \subseteq P$, let z be an element of Q, so $z = abn$ for some n in N. But a is in aN and bn is in bN. Therefore $z = (a)(bn)$ is in P. This shows that $Q \subseteq P$.

Hence $P = Q$.

Solution to Exercise 3.9

(a) There are three cosets of H in S_3:

$$A = \{e, (1\,2)\},\ B = \{(1\,2\,3), (1\,3)\} \text{ and } C = \{(1\,3\,2), (2\,3)\}.$$

(b) Consider the elements of B and C. We have

$$\underbrace{(1\,2\,3)}_{\in B}\underbrace{(1\,3\,2)}_{\in C} = e \in A, \text{ and}$$

$$\underbrace{(1\,3)}_{\in B}\underbrace{(2\,3)}_{\in C} = (1\,3\,2) \in C.$$

So the products of an element from B and an element from C are not necessarily in the same coset. This means that the product BC is not well defined.

Solution to Exercise 3.10

Remember that a subgroup of index 2 is always normal – see Exercise 3.3.

(a) $N = \{e, (1\,2\,3), (1\,3\,2)\}$

(b) The elements of G/N are $eN = N$ and $(1\,2)N = \{(1\,2), (1\,3), (2\,3)\}$. The Cayley table is below.

$\circ$	N	$(1\,2)N$
N	N	$(1\,2)N$
$(1\,2)N$	$(1\,2)N$	N

You may have used different notation for the second coset. This is fine.

Notice that another way of writing the Cayley table is

$\circ$	even	odd
even	even	odd
odd	odd	even

where 'even' stands for the coset containing the even permutations and 'odd' stands for the coset containing the odd permutations.

Solution to Exercise 4.1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Solution to Exercise 4.2

Since $r^4 = e$, we have $R = \langle r \rangle = \{e, r, r^2, r^3\}$. The Cayley table of R is as follows.

$\circ$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

Solution to Exercise 4.3

It is clear that ϕ is a function from $\mathbb{Z}$ to $2\mathbb{Z}$. We need to check that ϕ is a bijection and that it preserves the binary operation.

To check that ϕ is one–one, let $\phi(a) = \phi(b)$ for $a, b \in \mathbb{Z}$. Then $2a = 2b$, which implies that $a = b$. Therefore ϕ is one–one.

To show that ϕ is onto, let a be any element of $2\mathbb{Z}$. Then $a = 2m$ for some $m \in \mathbb{Z}$. Hence $a = \phi(m)$, proving that ϕ is onto.

Finally, we check that ϕ preserves the binary operation:

$$\begin{aligned}\phi(a+b) &= 2(a+b)\\ &= 2a + 2b\\ &= \phi(a) + \phi(b).\end{aligned}$$

Solution to Exercise 4.4

Since $aa^{-1} = e$ and ϕ is an isomorphism, we have that $\phi(a)\phi(a^{-1}) = \phi(e)$.

But $\phi(e)$ is the identity of H (by Theorem 4.3), so $\phi(a^{-1})$ behaves like the right inverse of $\phi(a)$ in H.

Now Proposition 1.6 gives that $\phi(a^{-1})$ is the inverse of $\phi(a)$ in H, that is,

$$(\phi(a))^{-1} = \phi(a^{-1}).$$

Solution to Exercise 4.5

In $\mathbb{Z}_5^*$ we have that $3^2 \equiv 4$, $3^3 \equiv 2$ and $3^4 \equiv 1$. Hence the element 3 is a generator of the group.

Since 1 is a generator of $\mathbb{Z}_4$, we might look for an isomorphism ϕ from $\mathbb{Z}_4$ to $\mathbb{Z}_5^*$ for which $\phi(1) = 3$.

The inverse of 1 in $\mathbb{Z}_4$ is 3 and the inverse of 3 in $\mathbb{Z}_5^*$ is 2, so we also need $\phi(3) = 2$. Since we know that we must have $\phi(0) = 1$, this leaves $\phi(2) = 4$.

Rewriting the Cayley table as

$\times_5$	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

we find that it does have the same pattern as the Cayley table for $(\mathbb{Z}_4, +_4)$, and so the function ϕ defined by

$$\phi(0) = 1, \phi(1) = 3, \phi(2) = 4, \phi(3) = 2$$

is an isomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_5^*$.

Solution to Exercise 4.6

(a) To show that the group H is abelian we must show that $xy = yx$ for any x and y in H.

Since ϕ is onto, for x and y in H there are elements a and b in G such that $\phi(a) = x$ and $\phi(b) = y$.

Now G is an abelian group, so $ab = ba$. Therefore, since ϕ is an isomorphism, we have

$$\begin{aligned} xy &= \phi(a)\phi(b) \\ &= \phi(ab) \\ &= \phi(ba) \\ &= \phi(b)\phi(a) \\ &= yx. \end{aligned}$$

Hence H is abelian.

(b) Since $\mathbb{Z}_6$ is an abelian group and S_3 is not, these groups cannot be isomorphic.

Solution to Exercise 4.7

Since $g^n = e$, the order of g must be finite by Definition 4.4. Suppose that the order of g is m. Then $m \leq n$, so by the Division Algorithm (Book A, Chapter 1, Theorem 4.1) there are $q, r \in \mathbb{N}$ with $n = qm + r$ and $0 \leq r < m$. Then, since $g^m = e$, we have $g^{qm} = e$, so that $e = g^n = g^{qm}g^r$ gives $g^r = e$. Since $r < m$, by definition of order we get $r = 0$. But then $n = qm$; that is, the order of g divides n, as required.

Solution to Exercise 4.8

Let $g \in G$, where $g \neq e$. Then by Proposition 4.5 the order of g must divide p. Since p is prime and we have assumed $g \neq e$, the order of g must be p. Hence G is cyclic and generated by g.

Solution to Exercise 4.9

Suppose that $\phi(a)$ has finite order n. By Proposition 4.2 the inverse ϕ^{-1} is an isomorphism, so by Theorem 4.6 $\phi^{-1}(\phi(a)) = a$ also has finite order n.

We have shown that if $\phi(a)$ has finite order, so does a. This is equivalent to showing that if a has infinite order, so does $\phi(a)$.

Solution to Exercise 4.10

(a) We know from the definition that ϕ is a function from $\mathbb{Z}$ to $\mathbb{Z}$. Furthermore, for all m and n in the domain $\mathbb{Z}$,

$$\phi(m+n) = 3(m+n) = 3m + 3n = \phi(m) + \phi(n).$$

Hence ϕ has the morphism property and so it is a homomorphism from $(\mathbb{Z}, +)$ to itself.

However, ϕ is not an isomorphism, since it is not onto. For example, the element 1 of the codomain is not in the image set of ϕ.

(b) The kernel consists of all elements that map to the identity of the codomain, which is 0. Thus it consists of all $n \in \mathbb{Z}$ such that

$$\phi(n) = 3n = 0.$$

The only possibility is $n = 0$. Thus

$$\mathrm{Ker}(\phi) = \{0\},$$

which is, trivially, a subgroup of the domain.

(c) The elements of the image are those integers of the form $\phi(n) = 3n$ for some $n \in \mathbb{Z}$. Hence

$$\mathrm{Im}(\phi) = \{3n : \ n \in \mathbb{Z}\} = 3\mathbb{Z}.$$

Now $3\mathbb{Z}$ is a non-empty set, since $0 \in 3\mathbb{Z}$. Also, if $3m$ and $3n$ are any two elements of $3\mathbb{Z}$, then

$$3m - 3n = 3(m-n) \in 3\mathbb{Z}.$$

Thus $3\mathbb{Z}$ is a subgroup of the codomain $\mathbb{Z}$, by Proposition 2.5.

Solution to Exercise 4.11

(a) Let $a, b \in \phi(G)$. Then $a = \phi(g)$ and $b = \phi(k)$ for some $g, k \in G$. Thus

$$ab = \phi(g)\phi(k) = \phi(gk) = \phi(kg) = \phi(k)\phi(g) = ba.$$

Hence $\phi(G)$ is abelian.

(b) Since g has order n, we know that $g^n = e_G$ and hence

$$(\phi(g))^n = \phi(g^n) = \phi(e_G) = e_H,$$

where e_G is the identity in G and e_H is the identity in H. The required result follows by Exercise 4.7.

Solution to Exercise 4.12

Let G be an abelian group. Then a quotient of G has the form G/N for some subgroup N of G (we know that since G is abelian, all its subgroups are normal).

By Theorem 4.15, there is a homomorphism ϕ from G onto the quotient group G/N. Since G is abelian, so is $\phi(G)$ by Exercise 4.11. But $\phi(G) \cong G/N$, which gives the required result.

Solution to Exercise 4.13

Firstly, we show that H contains N (and is thus non-empty). The coset $eN = N$ is the identity of the quotient group G/N and so is an element of the subgroup $\overline{H}$. Therefore, by the definition of H, we have $e \in H$ and so H is non-empty.

Furthermore, $nN = N$ for every $n \in N$. So, by the definition of H, we have $n \in H$ for every $n \in N$. Hence

$$N \subseteq H.$$

Now let a and b be elements of H. We will show that $a^{-1}b$ is in H. By the definition of H, the cosets aN and bN are elements of $\overline{H}$, which is a subgroup of G/N. It follows that $\overline{H}$ also contains

$$\begin{aligned}(aN)^{-1}(bN) &= (a^{-1}N)(bN)\\ &= (a^{-1}b)N.\end{aligned}$$

From the definition of H, this means that $a^{-1}b \in H$. Therefore $H \leq G$ by Proposition 2.4.

Solution to Exercise 5.1

(a) (i) $(1\,3)$; (ii) $(1\,4)(2\,3)$; (iii) $(1\,2)(3\,4)$; (iv) $(1\,2\,3\,4)$; (v) e.

(b) (i) $(1\,3)$; (ii) $(1\,4)(2\,3)$; (iii) $(1\,2)(3\,4)$; (iv) $(1\,4\,3\,2)$; (v) e.

Solution to Exercise 5.2

(i) By inspection we see that H_1 contains all the symmetries of Figure 5.2(c), hence it is a group under composition of permutations.

Similarly:

(ii) H_2 is the symmetry group for Figure 5.2(a), and the group of direct symmetries of Figure 5.2(e).

(iii) H_3 is the symmetry group for Figure 5.2(e).

(iv) H_4 is the symmetry group for Figure 5.2(b).

(v) H_5 is the symmetry group for Figure 5.2(d).

Solution to Exercise 5.3

We know from Example 5.1 that each left coset of H_3 in S_4 contains elements that are determined by where 2 maps *to*. Similarly, the elements of a given right coset of H_3 will be determined by the element that 2 maps *from*. More specifically:

- every element of $H_3(1\,2)$ sends 1 to 2
- every element of $H_3(2\,3)$ sends 3 to 2
- every element of $H_3(2\,4)$ sends 4 to 2.

Solution to Exercise 5.4

(a) The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24, so by Lagrange's Theorem these are the possible orders of the subgroups of S_4.

(b) One cycle structure is that of the identity. Only e has this cycle structure, and it has order 1. A complete answer is given in the table below.

Representative of cycle structure	Number of elements	Order
e	1 element	1
$(1\,2)$	6 elements	2
$(1\,2\,3)$	8 elements	3
$(1\,2\,3\,4)$	6 elements	4
$(1\,2)(3\,4)$	3 elements	2

(c) From part (b), we know that S_4 has

- one element of order 1
- nine elements of order 2
- eight elements of order 3
- six elements of order 4.

Solution to Exercise 5.5

(a) (i) $(2\,4)$ (ii) $(1\,3\,2\,4)$

(b) $g_1 = (1\,2\,4)$ or $(1\,2\,4\,3)$ or $(1\,4)$ or $(1\,4\,3)$;
$g_2 = (2\,3\,4)$ or $(1\,3\,2\,4)$ or $(1\,4\,3)$ or $(1\,2)$.

(c) There are five conjugacy classes, whose elements are described in the table in the solution to Exercise 5.4(b).

Solution to Exercise 5.6

(a) There are nine subgroups of order 2, each of them generated by a different element of order 2. On the other hand, each subgroup of order 3 contains two elements of order 3, so there are four such subgroups, each consisting of the identity and two elements of order 3:

$\{e, (1\,2\,3), (1\,3\,2)\}$,
$\{e, (1\,2\,4), (1\,4\,2)\}$,
$\{e, (1\,3\,4), (1\,4\,3)\}$,
$\{e, (2\,3\,4), (2\,4\,3)\}$.

(b) The cyclic subgroups of order 4 are those generated by an element of order 4, that is,

$\{e, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$,
$\{e, (1\,3\,2\,4), (1\,2)(3\,4), (1\,4\,2\,3)\}$,
$\{e, (1\,2\,4\,3), (1\,4)(2\,3), (1\,3\,4\,2)\}$.

(c) Since all the non-identity elements of V have order 2, V is not cyclic (no element can be a generator). Observe that $V = H_5$ in Exercise 5.2.

The subgroup V is isomorphic to all non-cyclic subgroups of order 4 in S_4, namely to $\{e, (1\,2), (3\,4), (1\,2)(3\,4)\}$ (note that this is H_4 in Exercise 5.2), $\{e, (1\,3), (2\,4), (1\,3)(2\,4)\}$, $\{e, (1\,4), (2\,3), (1\,4)(2\,3)\}$ and V itself.

Since any group of order 4 is either cyclic or isomorphic to V, these subgroups and the ones in part (b) are in fact all the subgroups of order 4.

(d) In Exercise 5.4 we saw that S_4 does not contain any elements of order 6, so S_4 does not contain a cyclic subgroup of order 6.

(e) The subgroup H_3 consists of those permutations in S_4 that fix the symbol 2 – that is, they map 2 to 2. We obtain isomorphic groups by considering the three sets that consist of those permutations that fix the symbols 1, 3 and 4 respectively:

$\{e, (2\,3), (2\,4), (3\,4), (2\,3\,4), (2\,4\,3)\}$,
$\{e, (1\,2), (1\,4), (2\,4), (1\,2\,4), (1\,4\,2)\}$,
$\{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

(f) There are no cyclic subgroups of S_4 of order 8 because S_4 has no elements of order 8.

If we represent the symmetries of a square as a group of permutations of the vertices of the square, we obtain a subgroup of S_4 with order 8, namely

$$D_4 = \{e, (1\,3), (2\,4), (1\,3)(2\,4), (1\,2)(3\,4), (1\,4)(2\,3), (1\,2\,3\,4), (1\,4\,3\,2)\}.$$

If we interchange the symbols 2 and 3 in each permutation in D_4 (this corresponds to ordering the vertices of the square in a slightly unnatural way!), we obtain another subgroup of order 8:

$$\{e, (1\,2), (3\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,3\,2\,4), (1\,4\,2\,3)\}.$$

Similarly, interchanging 3 and 4 in D_4 gives

$$\{e, (1\,4), (2\,3), (1\,4)(2\,3), (1\,2)(3\,4), (1\,3)(2\,4), (1\,2\,4\,3), (1\,3\,4\,2)\}.$$

(g) The subgroup A_4 of even permutations of S_4 has order 12.

Solution to Exercise 5.7

H_2 is the group of direct symmetries of the tetrahedron that fix vertex 2.
H_3 is the subgroup of $\Gamma(\text{TET})$ fixing vertex 2.
A_4 is the subgroup of direct symmetries of $\Gamma(\text{TET})$.

Solution to Exercise 5.8

(a) $(1\,2)H_3(1\,2)^{-1} = (1\,2)H_3(1\,2) = \{e, (2\,3), (2\,4), (3\,4), (2\,3\,4), (2\,4\,3)\}$.

$(1\,3\,2\,4)H_4(1\,3\,2\,4)^{-1} = (1\,3\,2\,4)H_4(1\,4\,2\,3) = H_4$.

(b) The subgroups H_4 and H_5 are not conjugate because $(1\,2) \in H_4$ is not conjugate to any element in H_5.

(c) No: for example, the subgroup $\{e, (1\,2)\}$ is not conjugate to $\{e, (1\,2)(3\,4)\}$.

(d) Yes. We have

$$(1\,2)\{e, (1\,3\,4), (1\,4\,3)\}(1\,2)^{-1} = \{e, (2\,3\,4), (2\,4\,3)\},$$
$$(1\,4)\{e, (2\,3\,4), (2\,4\,3)\}(1\,4)^{-1} = \{e, (1\,2\,3), (1\,3\,2)\},$$
$$(3\,4)\{e, (1\,2\,3), (1\,3\,2)\}(3\,4)^{-1} = \{e, (1\,2\,4), (1\,4\,2)\},$$
$$(2\,3)\{e, (1\,2\,4), (1\,4\,2)\}(2\,3)^{-1} = \{e, (1\,3\,4), (1\,4\,3)\}.$$

These conjugacy relations suffice to establish that all four subgroups of S_4 of order 3 are conjugate to one another.

Solution to Exercise 5.9

From Proposition 3.12, we know that a normal subgroup N of S_4 must be a union of conjugacy classes, which must include the class $\{e\}$. Therefore $|N|$ will be the sum of the sizes of these conjugacy classes. Moreover, by Lagrange's Theorem, this sum must divide 24.

We know from Exercise 5.4 that the conjugacy classes of S_4 have sizes 1, 3, 6 and 8. The only ways to add any of these numbers in such a way that one of the summands is 1 and the sum is a proper divisor of 24 are $1 + 3 = 4$ and $1 + 3 + 8 = 12$. Therefore a non-trivial normal subgroup of S_4 can only have size 4 or 12.

A normal subgroup of size 4 is the Klein subgroup $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. A normal subgroup of size 12 is the alternating group A_4.

Solution to Exercise 5.10

(a) Suppose that ϕ is a group homomorphism with domain S_4 and such that $\mathrm{Ker}(\phi) = A_4$. Then $S_4/A_4 \cong \mathrm{Im}(\phi)$ by the First Isomorphism Theorem.

Since $|A_4| = 12$, the index of A_4 in S_4 is 2; that is, $|S_4/A_4| = 2$. So $\mathrm{Im}(\phi)$ contains exactly two elements.

(b) The mapping $\phi : S_4 \to \mathbb{Z}_2$ defined by

$$\phi(\sigma) = \begin{cases} 0, & \text{if } \sigma \text{ is an even permutation,} \\ 1, & \text{otherwise} \end{cases}$$

is a homomorphism whose kernel is A_4.

Solution to Exercise 5.11

(a) Lagrange's Theorem gives 1, 2, 3, 4, 6 and 12 as possible orders of subgroups of A_4.

(b) A subgroup of A_4 is automatically a subgroup of S_4, so we seek those subgroups of S_4 that contain only even permutations. The trivial subgroup $\{e\}$ is one such subgroup, and it has order 1. Moreover, using the results in Exercise 5.6 we find

- three subgroups of order 2, such as $\{e, (1\,2)(3\,4)\}$
- four subgroups of order 3, such as $\{e, (1\,2\,3), (1\,3\,2)\}$
- the Klein subgroup V, of order 4
- the group A_4 itself, of order 12.

There is no subgroup of order 6, which shows that the converse of Lagrange's Theorem is false.

(c) We see by inspection that there is no element $g \in A_4$ such that $g(1\,2\,3)g^{-1} = (2\,3\,4)$. Therefore the permutations $(1\,2\,3)$ and $(2\,3\,4)$ are *not* conjugate in A_4.

Note that in S_4 there are three such g, namely $(1\,2\,3\,4), (1\,3\,2\,4)$ and $(1\,4)$, but these are odd permutations and hence not in A_4.

(d) There are four conjugacy classes in A_4, namely

$\{e\}$,
$\{(1\,2\,3), (1\,4\,2), (1\,3\,4), (2\,4\,3)\}$,
$\{(1\,3\,2), (1\,2\,4), (1\,4\,3), (2\,3\,4)\}$,
$\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

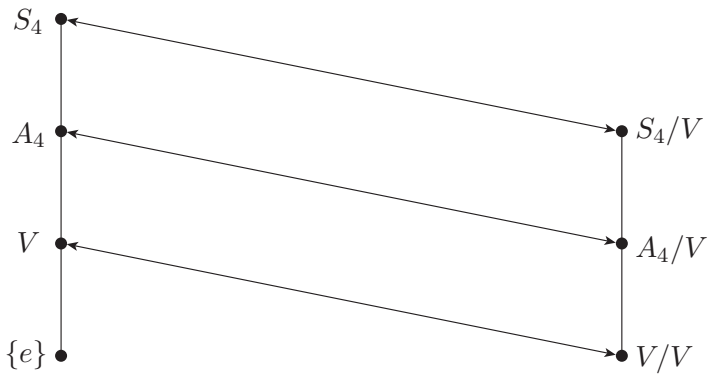
(e) The only non-trivial, proper normal subgroup of A_4 is the Klein subgroup V. Note that any subgroup of A_4 that is normal in S_4 will necessarily be normal in A_4.

Solution to Exercise 5.12

		S_4	A_4
(a)	order of group	24	12
(b)	number of subgroups of order 2	9	3
(c)	number of subgroups of order 3	4	4
(d)	number of cyclic subgroups of order 4	3	0
(e)	number of non-cyclic subgroups of order 4	4	1
(f)	number of cyclic subgroups of order 6	0	0
(g)	number of non-cyclic subgroups of order 6	4	0
(h)	number of subgroups of order 8	3	0
(i)	number of subgroups of order 12	1	1
(j)	total number of subgroups	30	10
(k)	total number of normal subgroups	4	3

Note that the trivial subgroup $\{e\}$ and the whole group are counted in parts (j) and (k).

Solution to Exercise 5.13



Chapter 6

Towards classification

Introduction

In this chapter we introduce two group-theoretic notions that are pivotal tools in classification results of the kind that we want to achieve. We also use these tools to obtain some initial results about the structure of cyclic groups and of finite abelian groups with certain special orders.

The first notion is a construction called *direct product*, which produces a new group from two (or more) given ones. In some cases, the newly constructed group shares some of the properties of its ancestors, such as being abelian or being cyclic. Under certain conditions, it is possible to decompose a given group as the direct product of two or more of its subgroups. This is often useful because knowledge of the (smaller) subgroups may give important information about the larger product group. We explore these concepts in Section 1.

In Section 2 we use direct products to describe the structure of finite cyclic groups. More specifically, we explain when a finite cyclic group can be written as a direct product of cyclic groups of smaller order. We also show that there is only one cyclic group of a given order, up to isomorphism.

Our preoccupation with cyclic groups is because they are the simplest examples of abelian groups, and it is finite abelian groups that we will eventually classify.

The second notion we introduce is one that you might have encountered in your previous studies: that of a group *acting on a set*. In Section 3 we remind you about group actions and the Orbit–Stabiliser Theorem, and we give a range of examples. Then we use group actions to prove two important results about finite groups.

One is *Cayley's Theorem*, which tells us that any finite group can be viewed as a subgroup of a suitable symmetric group S_n.

The other is *Cauchy's Theorem*, a partial converse to Lagrange's Theorem that tells us that a finite group of order n has an element of order p for each prime divisor p of n. Cauchy's Theorem is proved by considering a particular action of a group on tuples of its elements.

Finally, we obtain some results about expressing a finite group as a direct product of subgroups in the special cases of abelian groups whose order is either a product of prime numbers or the power of a prime.

One of our main goals in this book is to classify finite abelian groups. We will not be ready to fully prove this by the end of this chapter, but we will have made considerable progress in this direction.

Chapter guide

Sections 1 and 2 require roughly the same amount of study time.

Section 2 and the first part of Section 3 build on notions that should be familiar to you from your previous studies.

Section 3 is slightly longer and uses the tools provided in the first two sections to prove two pivotal results: Cayley's Theorem and Cauchy's Theorem.

All three sections contain a balanced mixture of examples and more abstract results.

1 Direct products

This section describes how to construct a group called the *direct product* of two given groups, and then describes certain conditions under which a group can be regarded as the direct product of its subgroups.

1.1 The external direct product of two groups

In this subsection, we introduce a method of constructing a new group from two existing ones: their *external direct product*. This method of construction will enable us to use existing groups as building blocks for larger ones. In turn, this will enable us to describe some groups in terms of smaller and possibly less complicated groups. This construction is, therefore, a key tool in our progress towards classifying groups.

First we need the notion of the **Cartesian product** of two sets: if X and Y are two sets, then the Cartesian product $X \times Y$ is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. For example, if $X = \{1, 2, 3\}$ and $Y = \{a, b\}$ then

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

When $X = Y$, the Cartesian product $X \times Y = X \times X$ is also denoted by X^2. More generally, the Cartesian product of n sets $X_1, X_2, \ldots, X_n$ is the set of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in X_i$ for all $i = 1, \ldots, n$.

In order to define the direct product of two groups, we need to specify the underlying set and a suitable binary operation. To understand how this is done, it will be useful to examine the familiar example of addition of vectors in the real plane $\mathbb{R} \times \mathbb{R}$ represented by the usual coordinate system.

Example 1.1 *Addition of vectors in* $\mathbb{R} \times \mathbb{R}$

We know that the real numbers with addition are a group, which we denoted by $(\mathbb{R}, +)$ in Chapter 5.

Each point in the plane is represented by an ordered pair (x, y) of real numbers. In other words, the coordinates of points in the plane are elements of the Cartesian product

$$\mathbb{R} \times \mathbb{R} = \{(x, y) : \ x \in \mathbb{R}, \ y \in \mathbb{R}\}.$$

The familiar operation of vector addition on $\mathbb{R} \times \mathbb{R}$ is defined as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Thus, vector addition is defined component by component in terms of addition in $\mathbb{R}$.

It turns out that $\mathbb{R} \times \mathbb{R}$ with addition defined as in Example 1.1 above is a group.

Exercise 1.1

Prove that the set $\mathbb{R} \times \mathbb{R}$ with the operation of vector addition is a group.

We can generalise the definitions of both the real plane as a Cartesian product and component-wise addition of real numbers.

Given two groups $(G, \circ)$ and $(H, *)$, we define the underlying set of a new group to be the Cartesian product of the sets G and H; that is, the set

In Example 1.1, $G = H = \mathbb{R}$.

$$G \times H = \{(g, h) : \ g \in G, \ h \in H\}.$$

As with $\mathbb{R} \times \mathbb{R}$, we can define an operation on this set by applying the original operations to the separate components. Generalising requires a little care because the operations for the two component groups may be different. As the first components come from G, with operation $\circ$, and the second components come from H, with operation $*$, the general definition of the new operation (which we call $\bullet$) is

In Example 1.1, $\bullet = \circ = * = +$.

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

Definition 1.2 *Direct product of two groups*

Let $(G, \circ)$ and $(H, *)$ be two groups. Their **direct product** $(G \times H, \bullet)$ is the group defined as follows.

Set The underlying set of the group is $G \times H$, the Cartesian product of the underlying sets G and H; that is,

$$G \times H = \{(g, h) : \ g \in G, \ h \in H\}.$$

Operation If (g_1, h_1) and (g_2, h_2) are elements of $G \times H$ then

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

This definition does indeed produce a group. Before we prove this, the following exercise will give you some 'hands-on' experience of direct products of groups.

Exercise 1.2

Write out the Cayley table of the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. Use $+$ for the new operation.

We are now ready to prove that the direct product of any two groups is indeed a group. The proof for the general case is similar to the solution to Exercise 1.1.

To verify that $(G \times H, \bullet)$ is a group, we must check the four group axioms.

To check that the above definition of $\bullet$ produces a closed binary operation on $G \times H$ (that is, it satisfies the closure axiom), we observe the following.

Let (g_1, h_1) and (g_2, h_2) be any two elements of $G \times H$. By the definition of $G \times H$, we know that g_1 and g_2 are elements of G and that h_1 and h_2 are elements of H.

Since G is a group, it is closed under the operation $\circ$, therefore $g_1 \circ g_2$ is in G. Since H is a group, it is closed under the operation $*$, so $h_1 * h_2$ is in H. Therefore, by the definition of $\bullet$, we have

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) \in G \times H.$$

The following exercise asks you to check the remaining group axioms for $(G \times H, \bullet)$.

Exercise 1.3

(a) Prove that $\bullet$ is associative (that is, check the associativity axiom).

(b) Let the identity of G be e_G and the identity of H be e_H. Prove that (e_G, e_H) is the identity of $G \times H$ (that is, check the identity axiom).

(c) Let (g, h) be an element of $G \times H$, where g has inverse g^{-1} in G and h has inverse h^{-1} in H. Prove that (g^{-1}, h^{-1}) is the inverse of (g, h) in $G \times H$ (that is, check the inverses axiom).

So far we have carefully distinguished the binary operations of the groups involved in the direct product construction. Now that we have shown that the direct product of two groups is a group, we revert to using either juxtaposition for the operations, or $+$ when both the operations are addition. Some texts refer to the **direct sum** of two groups, rather than direct product, when the groups are abelian and additive notation is used.

Exercise 1.4

Let G and H be abelian groups. Show that their direct product $G \times H$ is abelian.

1.2 Internal direct products

In some cases, a group is isomorphic to the direct product of two more of its subgroups. This is not always obvious, and in this subsection we investigate how to find out whether this is the case.

Consider the group of symmetries of the rectangle, $V = \{e, r, h, v\}$, where r is the half-turn about the centre and h and v are the reflections in the horizontal and vertical axes of symmetry. Recall also that $v = rh$. The Cayley table of V is as follows.

	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

We will show how V can be represented as a direct product of two smaller groups. More specifically, we will show that V is isomorphic to the direct product of two of its subgroups.

By Lagrange's Theorem (Chapter 5, Theorem 2.16) the only possible orders for subgroups of V are 1, 2 and 4. We aim to express V in the form $V = A \times B$, where A and B are subgroups of V. Now, by the definition of direct products of *any* two groups A and B,

$$|A \times B| = |A||B|.$$

Therefore if either A or B has order 1, then the other must have order 4 and is the whole group. However, this would not be expressing V as a product of smaller groups. Thus, it only makes sense to try to express V as the direct product of two subgroups of order 2. There are three subgroups of order 2, namely

$$H_1 = \{e, r\}, \quad H_2 = \{e, h\} \quad \text{and} \quad H_3 = \{e, v\}.$$

We pick H_1 and H_2, although any two of the three subgroups would do just as well. The Cayley table for $H_1 \times H_2$ is as follows.

	(e,e)	(r,e)	(e,h)	(r,h)
(e,e)	(e,e)	(r,e)	(e,h)	(r,h)
(r,e)	(r,e)	(e,e)	(r,h)	(e,h)
(e,h)	(e,h)	(r,h)	(e,e)	(r,e)
(r,h)	(r,h)	(e,h)	(r,e)	(e,e)

Since $rh = v$ in V, the Cayley table for V can be rewritten in the following way.

	e	r	h	rh
e	e	r	h	rh
r	r	e	rh	h
h	h	rh	e	r
rh	rh	h	r	e

You may have observed that these two tables have an entirely similar pattern. It follows that the function $\phi : H_1 \times H_2$ defined by

$$\phi : (x, y) \mapsto xy$$

is an isomorphism. Thus V can be represented as – that is, it is isomorphic to – the direct product of two of its subgroups. Since each of these subgroups is cyclic and of order 2, we can also say $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Not all attempts to decompose a group as a direct product of subgroups will work, as the following example shows.

Example 1.3 *A group that is not a non-trivial direct product*

The symmetric group S_3 has six elements:

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

This group is not abelian: consider, for example, the products $(1\,2)(1\,3)$ and $(1\,3)(1\,2)$.

If S_3 could be written as a *non-trivial* direct product – that is, as a direct product in which neither subgroup has order 1 – it would have to be as the direct product of subgroups of orders 2 and 3.

The group S_3 does possess subgroups of orders 2 and 3. For example, $H_1 = \{e, (1\,2)\}$ has order 2 and $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ has order 3.

However, any subgroup of order 2 is cyclic and is isomorphic to $\mathbb{Z}_2$. Equally, any subgroup of order 3 is cyclic and is isomorphic to $\mathbb{Z}_3$. It follows, therefore, that *any* attempt to form a direct product of such subgroups leads to a group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$, which is abelian by Exercise 1.4 and so not isomorphic to S_3.

Example 1.3 shows that, even if subgroups of suitable orders exist, a group may not be isomorphic to a direct product of these subgroups.

In fact, there are precise conditions under which a group is isomorphic to a direct product of two of its subgroups. These conditions form the content of Theorem 1.5 below.

We determine these conditions in two stages: first we establish necessary conditions on the subgroups and then we show that these conditions are also sufficient.

This discussion will be the proof of the first half of Theorem 1.5.

We start by showing that if a group G is the direct product of two of its subgroups, then there are certain restrictions on the subgroups.

So assume that H_1 and H_2 are subgroups of a group G and that $\phi : H_1 \times H_2 \to G$ defined by

$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism. We consider, in turn, the consequences of ϕ being onto, one–one and satisfying the morphism property.

The image set of ϕ consists of all products $h_1 h_2$ of an element of H_1 and an element of H_2. Hence, as ϕ is onto, every element of G is expressible in

this form. Using the notation $H_1H_2 = \{h_1h_2 : \ h_1 \in H_1, \ h_2 \in H_2\}$, this says that we must have $G = H_1H_2$. In other words, every element of G is the product of an element of H_1 with an element of H_2. Summing up, we have the following result.

If ϕ is an isomorphism, then $G = H_1H_2$.

Let us now look at the consequences of ϕ being one–one. Assume that $\phi(h_1, h_2) = \phi(k_1, k_2)$. Then we know that

$$(h_1, h_2) = (k_1, k_2),$$

which, by the definition of an ordered pair, implies that $h_1 = k_1$ and $h_2 = k_2$.

Strictly, the correct notation for expressions like $\phi(h_1, h_2)$ is $\phi((h_1, h_2))$. However, for ease of notation we will avoid double brackets where no ambiguity arises and simply write $\phi(h_1, h_2)$.

So $\phi(h_1, h_2) = \phi(k_1, k_2)$ means that $h_1h_2 = k_1k_2$. In other words, the fact that ϕ is one–one means that

$$h_1h_2 = k_1k_2 \quad \text{implies} \quad h_1 = k_1 \text{ and } h_2 = k_2.$$

Thus, because ϕ is one–one, each element of G can be expressed as a *unique* product of the form h_1h_2 with $h_1 \in H_1$ and $h_2 \in H_2$.

Exercise 1.5

Show that the fact that ϕ is one–one implies that $H_1 \cap H_2 = \{e\}$.

Hint: use the fact that $h = he = eh$ for any $h \in G$.

The result of the previous exercise tells us the following.

If ϕ is an isomorphism, then $H_1 \cap H_2 = \{e\}$.

For any two elements (h_1, h_2) and (k_1, k_2) of the direct product, the morphism property of ϕ gives

$$\begin{aligned}
&\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1, h_2)\phi(k_1, k_2) \\
&\Rightarrow \phi(h_1k_1, h_2k_2) = (h_1h_2)(k_1k_2) \\
&\Rightarrow h_1k_1h_2k_2 = h_1h_2k_1k_2 \\
&\Rightarrow k_1h_2 = h_2k_1, \qquad \text{using the left and right cancellation rules.}
\end{aligned}$$

What this means is that every element of H_1 commutes with every element of H_2.

We now show that we can deduce that H_1 is a normal subgroup of G. To do so, we show that $aH_1a^{-1} \subseteq H_1$ for each $a \in G$. Then H_1 is normal by Proposition 3.7 in Chapter 5.

So suppose that $a \in G$. Since we now know that $G = H_1H_2$, we can write $a = h_1h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.

Now, any element of aH_1a^{-1} is of the form aha^{-1}, where $h \in H_1$. So

$$\begin{aligned} aha^{-1} &= (h_1h_2)h(h_1h_2)^{-1} \\ &= h_1h_2hh_2^{-1}h_1^{-1} \\ &= h_1hh_2h_2^{-1}h_1^{-1} \qquad \text{(since } h \in H_1 \text{ and } h_2 \in H_2 \text{ commute)} \\ &= h_1hh_1^{-1} \in H_1 \qquad \text{(since } h, h_1, h_1^{-1} \in H_1\text{)}. \end{aligned}$$

Thus $aH_1a^{-1} \subseteq H_1$ as required.

The following exercise asks you to show that H_2 is also a normal subgroup of G.

Exercise 1.6

Prove that, for any $a \in G$,

$$aH_2a^{-1} \subseteq H_2.$$

Exercise 1.6 and the discussion preceding it give the following result.

If ϕ is an isomorphism, then both H_1 and H_2 are normal subgroups of G.

Summing up, if $\phi : H_1 \times H_2 \to G$ defined by

$$\phi : (h_1, h_2) \mapsto h_1h_2$$

is an isomorphism, then all three of the following conditions are satisfied:

(a) $G = H_1H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

This completes the proof of the first half of Theorem 1.5 below. Before we state the theorem and complete its proof, we introduce the standard terminology that is used when a group can be expressed as a direct product of subgroups.

Definition 1.4 *Internal direct product*

Let G be a group and let H_1 and H_2 be subgroups of G. Then G is the **internal direct product** of H_1 and H_2 if the map

$$\begin{aligned} \phi &: H_1 \times H_2 \to G \\ \phi &: (h_1, h_2) \mapsto h_1h_2 \end{aligned}$$

is an isomorphism.

The direct product $H_1 \times H_2$ in Definition 1.4 is 'internal' in that H_1 and H_2 are subgroups of G. The next theorem gives necessary and sufficient

conditions for a group to be the internal direct product of two given subgroups.

Theorem 1.5 *Internal Direct Product Theorem*

If H_1 and H_2 are subgroups of a group G, then

$$\phi : H_1 \times H_2 \to G$$
$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

In particular, when these three conditions are satisfied, G is the internal direct product of H_1 and H_2.

Proof As remarked above, we have proved that the conditions are necessary; that is, we have proved that if ϕ is an isomorphism, then the three conditions hold. For sufficiency, we need to prove that, if the three conditions hold, then ϕ is an isomorphism.

The three conditions, in turn, give that ϕ is onto, one–one and has the morphism property.

To see that ϕ is onto, recall that $G = H_1 H_2$. Then every $g \in G$ can be written as $g = h_1 h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$. Hence $g = \phi(h_1, h_2)$ and ϕ is onto.

We now check that ϕ is one–one. Suppose that

$$\phi(h_1, h_2) = \phi(k_1, k_2).$$

Then $h_1 h_2 = k_1 k_2$ for $h_1, k_1 \in H_1$ and $h_2, k_2 \in H_2$. So

$$k_1^{-1} h_1 = k_2 h_2^{-1}.$$

But the left-hand side is an element of H_1 and the right-hand side is an element of H_2. Since both sides are equal, they belong to both H_1 and H_2 and, hence, to the intersection $H_1 \cap H_2$.

However, $H_1 \cap H_2 = \{e\}$.

Thus $k_1^{-1} h_1 = k_2 h_2^{-1} = e$.

It follows that $h_1 = k_1$ and $h_2 = k_2$, and so $(h_1, h_2) = (k_1, k_2)$. Thus ϕ is one–one.

Checking the morphism property is slightly more involved. Let (h_1, h_2) and (k_1, k_2) be elements of $H_1 \times H_2$. We want to show that

$$\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1, h_2)\phi(k_1, k_2).$$

But $\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1 k_1, h_2 k_2) = h_1 k_1 h_2 k_2$, and
$\phi(h_1, h_2)\phi(k_1, k_2) = h_1 h_2 k_1 k_2$,

so the morphism property in this case is equivalent to

$$h_1k_1h_2k_2 = h_1h_2k_1k_2;$$

that is, after using the cancellation laws, to

$$k_1h_2 = h_2k_1.$$

Now consider the product

$$k_1h_2k_1^{-1}h_2^{-1} \in G.$$

Since h_2 is in H_2, so is h_2^{-1}. Since H_2 is normal in G, we have that $k_1h_2k_1^{-1}$ is in H_2. Therefore $k_1h_2k_1^{-1}h_2^{-1}$ is in H_2.

Similarly, $h_2k_1^{-1}h_2^{-1} \in H_1$, so $k_1h_2k_1^{-1}h_2^{-1} \in H_1$.

Therefore $k_1h_2k_1^{-1}h_2^{-1} \in H_1 \cap H_2$. But since $H_1 \cap H_2 = \{e\}$, we have

$$k_1h_2k_1^{-1}h_2^{-1} = e,$$

which is equivalent to $k_1h_2 = h_2k_1$, and therefore also to the morphism property.

This concludes the proof that if conditions (a), (b) and (c) hold, then ϕ is an isomorphism. ■

Theorem 1.5 gives another reason why S_3 is not the direct product of two subgroups isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$: while $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ is a normal subgroup of order 3, we know that S_3 has no normal subgroup of order 2.

Exercise 1.7

Consider the cyclic group $\mathbb{Z}_6$ and denote its underlying set by $\{e, a, a^2, a^3, a^4, a^5\}$. Show that $\mathbb{Z}_6$ has normal subgroups of orders 2 and 3 that satisfy the conditions of Theorem 1.5. Deduce that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

The result you are asked to prove in the following exercise is implicit in the proof of the morphism property for ϕ in Theorem 1.5: in any internal direct product $G \cong H \times K$, the subgroups H and K satisfy a commutativity condition, in the sense that every element of H commutes with every element of K.

Exercise 1.8

Let $G \cong H \times K$ be the internal direct product of subgroups H and K of G. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

Let G and H be two groups with identities e_G and e_H respectively. Then the set

$$\widehat{G} = \{(g, e_H) : g \in G\}$$

is the subset of the direct product $G \times H$ that contains all pairs where the second element is the identity in H. It is not difficult to show – though we will not do so here – that $\widehat{G}$ is a subgroup of $G \times H$ that is isomorphic to G. Similarly, the set

$$\widehat{H} = \{(e_G, h) : h \in H\}$$

forms a subgroup of $G \times H$ that is isomorphic to H.

Then the direct product $G \times H$ is also the internal direct product of its subgroups $\widehat{G}$ and $\widehat{H}$. Thus, the distinction between the external and internal direct products of two groups is simply an indication of whether we regard the factor groups as subgroups of the product group. In the rest of Book B we will usually drop this distinction and simply refer to a *direct product* even when we work with an internal direct product.

Before we move on, it will be useful to consider direct products of more than two groups.

Theorem 1.6

If A, B and C are groups, then:

(a) $A \times B \cong B \times A$

(b) $A \times (B \times C) \cong (A \times B) \times C$.

Proof

(a) Consider the function $\phi : A \times B \to B \times A$ defined by

$$\phi : (a, b) \mapsto (b, a).$$

We claim that ϕ is an isomorphism.

To show that ϕ is one–one, suppose that $\phi(a_1, b_1) = \phi(a_2, b_2)$. Then $(b_1, a_1) = (b_2, a_2)$ by the definition of ϕ. Hence $b_1 = b_2$ and $a_1 = a_2$ by the definition of ordered pairs, and so

$$(a_1, b_1) = (a_2, b_2),$$

which shows that ϕ is one–one.

If (b, a) is any element of the codomain $B \times A$, then $b \in B$ and $a \in A$, so $(a, b) \in A \times B$ and $\phi(a, b) = (b, a)$. Hence ϕ is onto.

To check the morphism property, let (a_1, b_1) and (a_2, b_2) be any two elements of $A \times B$. Then

$$\begin{aligned} \phi((a_1, b_1)(a_2, b_2)) &= \phi(a_1 a_2, b_1 b_2) \\ &= (b_1 b_2, a_1 a_2) \\ &= (b_1, a_1)(b_2, a_2) \\ &= \phi(a_1, b_1)\phi(a_2, b_2). \end{aligned}$$

This completes the proof that $A \times B \cong B \times A$.

(b) You are asked to prove the second part of the theorem in the following exercise. ■

Exercise 1.9

Show that the function

$$\begin{aligned} \psi : A \times (B \times C) &\to (A \times B) \times C \\ \psi : \quad (a, (b, c)) &\mapsto \quad ((a, b), c) \end{aligned}$$

is an isomorphism.

The first part of Theorem 1.6 says that if we alter the order of the factor groups in a direct product, we obtain an isomorphic group.

The second part of Theorem 1.6 says that the bracketing of terms in a direct product of three (or more) groups is unnecessary.

So, just as for, say, the multiplication of integers, these 'commutative' and 'associative' laws mean that a direct product of two or more groups may be written in any order, without the need for brackets, since all such expressions produce isomorphic groups. Theorems 1.5 and 1.6 give us the following result concerning the direct product of a finite number of subgroups of a group G. The full proof is omitted.

Corollary 1.7

If H_i are subgroups of a group G for $i = 1, \ldots, n \in \mathbb{N}$, $n \geq 2$, then

$$\begin{aligned} \phi\colon \quad H_1 \times H_2 \times \cdots \times H_n &\to G \\ \phi : (h_1, h_2, \ldots, h_n) &\mapsto h_1 h_2 \cdots h_n \end{aligned}$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2 \cdots H_n$

(b) $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$ for $1 \leq i \leq n$

(c) $H_1, H_2, \ldots, H_n$ are normal subgroups of G.

In particular, when these three conditions are satisfied, G is the internal direct product of $H_1, H_2, \ldots, H_n$.

Notice that condition (b) is stronger than requiring that $H_i \cap H_j = \{e\}$ for $i \neq j$. The next example shows that this extra strength is needed.

Example 1.8 *The Klein group*

Let G be the Klein group,

$$G = \Gamma(\square) = \{e, r, h, v\}.$$

Let $H_1 = \{e, r\}, H_2 = \{e, h\}$ and $H_3 = \{e, v\}$. Then:

- $e = eee$, $r = ree$, $h = ehe$ and $v = eev$ and so condition (a) from Corollary 1.7 holds
- $H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3 = \{e\}$
- since G is abelian, H_1, H_2, H_3 are all normal in G.

However $G \ncong H_1 \times H_2 \times H_3$, since the order of G is 4, whereas the order of $H_1 \times H_2 \times H_3$ is 8.

Note that condition (b) in Corollary 1.7 does not hold here, since

$$H_1 \cap H_2 H_3 = H_1 \cap \{e, h, v, r\} = \{e, r\}.$$

When a group G has two subgroups H and K with trivial intersection, we can say quite a lot about the product HK and its relation to the direct product $H \times K$.

Recall that $HK = \{hk : h \in H \text{ and } k \in K\}$.

Proposition 1.9

Let G be a group with subgroups H and K such that $H \cap K = \{e\}$. Then:

(a) If H and K have finite orders r and s respectively, then HK has rs distinct elements. In particular, if $rs = |G|$ then $G = HK$.

(b) If $kh = hk$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G with $HK \cong H \times K$.

Proof

(a) Suppose that $h_1 k_1 = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$h_2^{-1} h_1 = k_2 k_1^{-1} = e$$

since $H \cap K = \{e\}$. Thus $h_2 = h_1$ and $k_2 = k_1$. This means that HK must have $|H| \times |K| = rs$ distinct elements.

(b) We first apply the subgroup criterion in Proposition 2.4 of Chapter 5 to show that HK is a subgroup of G. It is clear that HK is non-empty, so we only need to check that for any elements x, $y \in HK$ the product $x^{-1}y$ is again in HK.

Suppose $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned} x^{-1}y &= (h_1k_1)^{-1}h_2k_2 \\ &= k_1^{-1}h_1^{-1}h_2k_2 \\ &= h_1^{-1}h_2k_1^{-1}k_2, \end{aligned}$$

since elements of H commute with elements of K.

But $h_1^{-1}h_2 \in H$ and $k_1^{-1}k_2 \in K$ (because H and K are both subgroups), therefore the product $h_1^{-1}h_2k_1^{-1}k_2 = x^{-1}y$ is in HK, as required.

Thus HK is a subgroup of G.

Now, since $hk = kh$ for all $h \in H$ and $k \in K$, we have

$$\begin{aligned} hkh^{-1} &= k \in K \quad \text{and} \\ khk^{-1} &= h \in H, \end{aligned}$$

so H and K are both normal subgroups of HK.

Hence, since $H \cap K = \{e\}$, we can apply Theorem 1.5 with $HK = G$ to show that $HK \cong H \times K$ as required. ■

The next exercise gives a useful tip for working with direct products of two groups inside abelian groups.

Exercise 1.10

Let G be an abelian group, and let H_1, H_2 be subgroups of G with

$$H_1 \cap H_2 = \{1\}.$$

Show that if $h_1 \in H_1$ and $h_2 \in H_2$ are such that $h_1h_2 = 1$, then $h_1 = 1$ and $h_2 = 1$.

Finally, we include a result about direct products of direct products.

Proposition 1.10

Let H, K be subgroups of G, and H_1, H_2 be subgroups of H. Suppose that $G \cong H \times K$ and $H \cong H_1 \times H_2$. Then $G \cong H_1 \times H_2 \times K$.

Proof We show that the three conditions in Corollary 1.7 hold for G, H_1, H_2 and K.

(a) Since $G \cong H \times K$, we have that $G = HK$ and since $H \cong H_1 \times H_2$, we have that $H = H_1H_2$. It follows that $G = H_1H_2K$.

(b) Since $G \cong H \times K$, we have that $H \cap K = \{e\}$ and so $H_1H_2 \cap K = \{e\}$.

Since $H \cong H_1 \times H_2$, we have $H_1 \cap H_2 = \{e\}$. Suppose $g \in H_1K \cap H_2$. Then

$$g = h_1k = h_2 \qquad (*)$$

for some $h_1 \in H_1, h_2 \in H_2$ and $k \in K$.

But then $k = h_1^{-1}h_2 \in H$ and so $k \in H \cap K$. Thus $k = e$, and $h_1 = h_2$. But $h_1 = h_2$ implies that $h_1 = h_2 = e$ because $H_1 \cap H_2 = \{e\}$. Then equation $(*)$ implies $g = e$, and so

$$H_1K \cap H_2 = \{e\}.$$

The proof that $H_2K \cap H_1 = \{e\}$ is similar.

(c) Since $G \cong H \times K$, by Theorem 1.5 we have that K is normal in G. From Exercise 1.8 we know that:

- $hk = kh$ for all $h \in H$ and $k \in K$
- $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$.

Now let $h \in H_1$ and $g \in G$. We can write $g = h_1h_2k$ for some $h_1 \in H_1, h_2 \in H_2$ and $k \in K$. Then

$$\begin{aligned} ghg^{-1} &= h_1h_2khk^{-1}h_2^{-1}h_1^{-1} \\ &= h_1h_2h_2^{-1}kk^{-1}hh_1^{-1} \\ &= h_1hh_1^{-1} \in H_1. \end{aligned}$$

Thus H_1 is normal in G. Similarly, H_2 is normal in G.

We have shown that the three conditions in Corollary 1.7 are satisfied and hence that $G \cong H_1 \times H_2 \times K$. ■

2 Cyclic groups

We defined cyclic groups in Subsection 1.4 of Chapter 5. This section describes the key properties of their structure, starting with a complete description of all cyclic groups.

We will often retain multiplicative notation despite the fact that we know that cyclic groups are abelian.

2.1 The classification of cyclic groups

We are already in a position to describe fully all cyclic groups up to isomorphism. We do so by showing that any cyclic group is isomorphic to one of a list of concrete examples of groups. In fact, the concrete examples are

$$(\mathbb{Z}, +) \quad \text{and} \quad (\mathbb{Z}_n, +_n)$$

for each positive integer n.

$\mathbb{Z}$ is also generated by -1.

The cyclic group with which you are most familiar is $(\mathbb{Z}, +)$, which is generated by the element 1.

Theorem 2.1

(a) All infinite cyclic groups are isomorphic to $(\mathbb{Z}, +)$.

(b) A finite cyclic group of order n is isomorphic to the quotient group $\mathbb{Z}/n\mathbb{Z}$, which is $(\mathbb{Z}_n, +_n)$.

Proof

(a) Let G be an infinite cyclic group. Then G has a generator, a say, so every element of G can be written as a^n for some $n \in \mathbb{Z}$.
Define the function $\phi : G \to \mathbb{Z}$ by

$$a^n \mapsto n.$$

We claim that ϕ is an isomorphism. Since $a^n = a^m \Rightarrow n = m$, we have that ϕ is well defined. For any $m \in \mathbb{Z}$, $\phi(a^m) = m$, so ϕ is onto.

Since $\phi(a^n) = \phi(a^m) \Rightarrow n = m$, we have that

$$\phi(a^n) = \phi(a^m) \Rightarrow a^n = a^m,$$

so ϕ is one–one.

Finally, we check the morphism property, that is, we check that $\phi(a^n) + \phi(a^m) = \phi(a^n a^m)$. The key to this is that we have been using standard power notation when considering elements of groups; that is, we write

$$\underbrace{aa\cdots a}_{n \text{ times}} \text{ as } a^n, \quad \text{and} \quad \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}} \text{ as } a^{-n}.$$

Thus, the familiar power laws apply to products of elements of G, and we get

$$\phi(a^n) + \phi(a^m) = n + m = \phi(a^{n+m}) = \phi(a^n a^m).$$

Therefore the morphism property holds.

(b) Let G be a finite cyclic group of order n. Then G has a generator, a say, so every element of G can be written as a^s for some $s \in \mathbb{Z}$ and, moreover, $a^n = e$.

Now, by the Division Algorithm (see Book A, Chapter 1, Theorem 4.1) we have that $s = kn + r$ where $0 \leq r < n$. Thus

$$a^s = a^{kn+r} = (a^n)^k a^r = a^r.$$

Hence $G = \{e, a, a^2, \ldots, a^{n-1}\}$, and these elements are distinct.

Define the function $\phi : G \to \mathbb{Z}/n\mathbb{Z}$ by

$$a^r \mapsto r + n\mathbb{Z}.$$

We show that ϕ is an isomorphism. It is clear that ϕ is onto. To show that ϕ is one–one, we need to check that $\phi(a^r) = \phi(a^s) \Rightarrow a^r = a^s$. Now

$$\begin{aligned}\phi(a^r) = \phi(a^s) &\Rightarrow r + n\mathbb{Z} = s + n\mathbb{Z} \\ &\Rightarrow r - s = kn \text{ for some } k \in \mathbb{Z} \\ &\Rightarrow r = s + kn \\ &\Rightarrow a^r = a^{s+kn} = a^s a^{kn} = a^s \ \ (\text{since } a^n = e),\end{aligned}$$

as required.

Finally, we need to show the morphism property. Suppose that $r, s \in \mathbb{Z}$. Let $t \in \mathbb{Z}$ be such that $0 \leq t < n$ and $t \equiv r + s \pmod{n}$. Then

$$\begin{aligned}\phi(a^r a^s) &= \phi(a^{r+s}) \\ &= \phi(a^t) \qquad (\text{since } r + s = t + kn \text{ for some } k \in \mathbb{Z}) \\ &= t + n\mathbb{Z} \\ &= r + n\mathbb{Z} + s + n\mathbb{Z} \\ &= \phi(a^r) + \phi(a^s),\end{aligned}$$

so the morphism property holds. ■

2.2 Subgroups and quotient groups of cyclic groups

Chapter 5 showed that subgroups and quotient groups of abelian groups are abelian. A natural question arises as to whether the same is true if 'abelian' is replaced by 'cyclic'. The answer is yes, as will be shown in this subsection.

Although we know, from Theorem 2.1, that cyclic groups can be written in a specific form, namely as $\mathbb{Z}$ or $\mathbb{Z}_n$, it is sometimes convenient to view them in a more abstract way and in multiplicative notation. This more abstract view is adopted in this subsection.

We begin by looking at quotients of cyclic groups.

Theorem 2.2 *Quotients of cyclic groups*

(a) Let G be a cyclic group and let $\phi : G \to H$ be a homomorphism. Then $\phi(G)$ is cyclic.

(b) Let G be a cyclic group generated by a and let H be a subgroup of G. Then the quotient group G/H is cyclic and generated by the coset aH.

Proof

(a) Since G is cyclic, it has a generator g, say. We claim that $\phi(g) \in H$ generates $\phi(G)$.

Let $h \in \phi(G)$. Then $h = \phi(a)$ for some $a \in G$. Since g generates G we know that $a = g^n$ for some $n \in \mathbb{Z}$. Hence

$$h = \phi(a) = \phi(g^n) = (\phi(g))^n.$$

Thus we have shown that every element of $\phi(G)$ can be written in the form $(\phi(g))^n$ for some $n \in \mathbb{Z}$, and so $\phi(G)$ is cyclic with generator $\phi(g)$, as required.

(b) We must show that every element of G/H is of the form $(aH)^k$ for some $k \in \mathbb{Z}$.

Suppose that gH is any element of G/H. Then, since G is generated by a, we know that $g = a^k$ for some integer k. But $(aH)^k = (a^k)H = gH$. Hence aH generates G/H. ■

Before proving that every subgroup of a cyclic group is cyclic, you are asked to work through an exercise that should help you understand what is happening.

Exercise 2.1

Let G be a cyclic group generated by a and let H be a non-trivial subgroup of G. Each element of H must be of the form a^k with $k \geq 0$. Among the elements of H, choose the one with the smallest non-zero exponent and let this exponent be m. Since H is non-trivial, such an m exists.

(a) Suppose that a^k is an element of H. Show that m divides k and hence that $H = \langle a^m \rangle$.

Assume now that G is a finite cyclic group of order n – that is, a has order n.

(b) Deduce that m divides n.

(c) If $n = mq$, show that the order of H is q.

Hint: in part (a), use the Division Algorithm (Book A, Chapter 1, Theorem 4.1).

Exercise 2.1 is a major step towards the proof that every subgroup of a cyclic group is cyclic.

Theorem 2.3

Let G be a cyclic group and let H be a subgroup of G. Then H is cyclic.

Proof If H is the trivial subgroup, that is $H = \{e\}$, then H is generated by e and so it is cyclic.

We therefore consider the case when $H \neq \{e\}$, so that H contains a^t for some integer $t \neq 0$. Then H also contains $a^{-t} = (a^t)^{-1}$. As one of t and $-t$ must be positive, H contains a^k for some positive integer k and we can choose m to be the least such positive integer. Then $H = \langle a^m \rangle$ by Exercise 2.1, and so H is cyclic and generated by a^m. ■

Interpreting this result for the infinite cyclic group $\mathbb{Z}$, using additive notation, gives the following corollary.

Corollary 2.4

The subgroups of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$, $n \geq 0$.

Proof By Theorem 2.3, every subgroup of $\mathbb{Z}$ is cyclic. The cyclic subgroups of $\mathbb{Z}$ are those generated by an element of $\mathbb{Z}$, that is, those of the form $\{nz : z \in \mathbb{Z}\} = n\mathbb{Z}$ for some $n \in \mathbb{Z}, n > 0$, as required. ■

We can summarise the results in Exercise 2.1 and Theorem 2.3 as follows. If

$$G = \langle a : a^n = e \rangle$$

is a finite cyclic group of order n and H is a subgroup of G, then:

- H is cyclic
- H is generated by a^m, where m is the smallest positive exponent of a such that $a^m \in H$
- m divides n
- if $n = mq$ then H has order q.

We have shown that every subgroup of a cyclic group is also cyclic. In fact where the group is finite, we will do rather more. As we have seen, Lagrange's Theorem states that, for finite groups, the order of a subgroup must divide the order of the group. For finite *cyclic* groups we can prove a strong converse to Lagrange's Theorem: for every divisor of the order of the group, not only is there a subgroup having that number of elements, but also this subgroup is unique.

Theorem 2.5 *Subgroups of cyclic groups*

Let $G = \langle a \rangle$ be a finite cyclic group of order n, so that a has order n. If q is a factor of n with $n = mq$, then G has a unique subgroup of order q that is generated by the element a^m.

Proof

We start by proving the existence of subgroups whose orders correspond to factors of the order of the group.

Let H be the subgroup $H = \langle a^m \rangle$. In Exercise 2.1, you showed that the order of H is q. Thus, given a factor q of n, the subgroup generated by a^m, where $n = mq$, has order q.

Finally, we show that the subgroup corresponding to the factor q of n is unique.

Suppose that $n = mq$. Then we know that there *is* a subgroup $\langle a^m \rangle$ of order q. Let H be any subgroup of order q. From Exercise 2.1 and Theorem 2.3, we know that H is cyclic and generated by a^l, where l is the least positive exponent of a occurring among the elements of H. Furthermore, the order of H is k, where $n = lk$. But the order of H is q, so $k = q$ and $mq = n = lk = lq$, and, therefore, $m = l$. Thus H is the subgroup generated by a^m.

This completes the proof of Theorem 2.5. ■

Theorem 2.5 can be regarded as a strong converse to Lagrange's Theorem for cyclic groups. We say 'strong' because not only is there a subgroup for every factor of the order of the group, but, in addition, this subgroup is unique.

Later we will investigate the effect of relaxing the assumptions about the group G. We will first consider the case where G is finite and abelian (instead of cyclic) and then go on to relax the condition further to merely finite. At each stage we will still obtain some sort of converse to Lagrange's Theorem; but, as the conditions on G are relaxed, the conclusions become weaker, although still useful.

We conclude this subsection by interpreting the results that we have obtained so far for our standard finite cyclic groups, that is, the groups $\mathbb{Z}_n$.

At this point, a word is in order about how we think of $\mathbb{Z}_n$. In Theorem 2.1, the group $\mathbb{Z}_n$ was defined as the quotient group $\mathbb{Z}/n\mathbb{Z}$. However, in practice we think of $\mathbb{Z}_n$ as the set $\{0, 1, \ldots, n-1\}$, with addition carried out modulo n.

Since the order of $\mathbb{Z}_n$ is n, by Theorem 2.5 there is a subgroup corresponding to each factor of n. That is, if q is a factor of n, then $\mathbb{Z}_n$ has a cyclic subgroup of order q. Theorem 2.1 tells us that this subgroup must be isomorphic to $\mathbb{Z}_q$.

Moreover, we know a generator of the subgroup. Since $\mathbb{Z}_n$ is generated by 1, the subgroup of order q is generated by $m = \frac{n}{q}$.

Exercise 2.2

(a) Write down the orders of the subgroups of $\mathbb{Z}_{24}$.

(b) For each such subgroup:

(i) state to which $\mathbb{Z}_k$ it is isomorphic

(ii) by using the remark above about how we think of the groups $\mathbb{Z}_n$, give an explicit list of its elements.

The interpretation of our results about quotient groups is also seen quite easily: for each factor q of n, there is a subgroup of $\mathbb{Z}_n$ of order q. This subgroup is normal. The corresponding quotient group is cyclic, by Theorem 2.2, and it has order

$$\frac{|\mathbb{Z}_n|}{q} = \frac{n}{q}.$$

Hence the quotient group $\mathbb{Z}_n/\mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{\frac{n}{q}}$.

2.3 Direct products of cyclic groups

In this subsection we will apply the direct product ideas from Section 1 of this chapter to cyclic groups.

We recall some terminology and results about integers. You saw the details in Book A, Chapter 1, Section 4, so here we restate the results that we need without proof.

Let m and n be two positive integers and let $p_1, p_2, \ldots, p_k$ be the prime numbers occurring in either of their prime factorisations. Then

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$

where a_i or b_i, but not both, might be zero.

For example, if $m = 126$ and $n = 120$ then $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ and we have

$$126 = 2 \times 3^2 \times 5^0 \times 7 \text{ and } 120 = 2^3 \times 3 \times 5 \times 7^0.$$

We know that the prime factorisation of mn is

$$p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k},$$

so if p is a prime factor of mn, then p must be a prime factor of either m or n or both.

Recall that the **highest common factor** of m and n, written $\text{hcf}(m, n)$, is the largest positive integer h that is a factor of both. If c_i is the smaller of a_i and b_i for each i, then h has prime factorisation

$$p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}.$$

For example, $\text{hcf}(126, 120) = 2^1 \times 3^1 \times 5^0 \times 7^0 = 2 \times 3 = 6$.

The **least common multiple** of m and n, written $\text{lcm}(m, n)$, is the smallest positive integer l that is a multiple of both m and n. If d_i is the larger of a_i and b_i for each i, then l has prime factorisation

$$p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$

For example, $\text{lcm}(126, 120) = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520$.

Two positive integers m and n are said to be **coprime** if their highest common factor is 1.

Proposition 2.6

Let m and n be two positive integers and let $h = \text{hcf}(m, n)$ and $l = \text{lcm}(m, n)$. Then:

(a) The product of m and n is the product of their highest common factor and least common multiple, that is, $mn = hl$.

(b) If m and n are coprime then their least common multiple is mn.

(c) There are integers a and b such that $am + bn = \text{hcf}(a, b)$. In particular, if m and n are coprime there are integers a and b such that $am + bn = 1$.

This proposition combines the results from Proposition 4.7, Lemma 4.9 and Proposition 4.15 of Book A, Chapter 1.

The results in Proposition 2.6 turn out to be relevant when we calculate the order of the element of a direct product. You can tackle the following exercise using direct calculation, but we will shortly prove a result that will avoid the need for calculations.

Exercise 2.3

(a) What is the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$?

(b) What is the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$?

As promised, we now prove some results that enable us to avoid direct calculations when determining the order of an element in a direct product. The following lemma concerns the order of two commuting elements in any group.

Lemma 2.7

Let a and b be elements of finite orders m and n respectively in a group G. Suppose that $ba = ab$ and that $\langle a \rangle \cap \langle b \rangle = \{e\}$ (that is, the only element of G that can be written both as a power of a and as a power of b is e).

Then the order of ab is the least common multiple of m and n.

Proof Let $l = mp = nq$ be the least common multiple of m and n. Since a and b commute, we have that $(ab)^r = a^r b^r$ for any integer r. Then

$$(ab)^l = a^l b^l = a^{mp} b^{nq} = (a^m)^p (b^n)^q = e^p e^q = e,$$

so the order of ab is at most l. Now let $k > 0$ and suppose that $(ab)^k = e$. Then $a^k b^k = e$ so $a^k = b^{-k}$. But then $a^k \in \langle a \rangle \cap \langle b \rangle$ so $a^k = e$. Similarly, $b^k = e$. By Proposition 4.5 of Chapter 5, we have that k is a common multiple of m and n, and so $k \geq l$. Thus the order of ab is at least l. We have already seen that the order of ab is at most l, so it must be l. ■

Exercise 2.4

Let G be an abelian group and let $g_1, g_2, \ldots, g_r$ be elements of G that have distinct prime orders $p_1, p_2, \ldots, p_r$ respectively. Show that the order of $g_1 g_2 \cdots g_r$ is $p_1 p_2 \cdots p_r$.

Proposition 2.8

Let G, A, B be groups with $G = A \times B$. Suppose that $a \in A$ has order m and $b \in B$ has order n. Then the order of (a, b) is the least common multiple of m and n.

Proof We consider the elements (a, e) and (e, b) in $A \times B$ and check the hypotheses of Lemma 2.7. Firstly, $(a, e)(e, b) = (a, b) = (e, b)(a, e)$. Secondly $\langle (a, e) \rangle = \{(a^k, e) : k = 0, \ldots, m-1\}$ and $\langle (e, b) \rangle = \{(e, b^k) : k = 0, \ldots, n-1\}$, so that

$$\langle (a, e) \rangle \cap \langle (e, b) \rangle = \{(e, e)\}.$$

Since both hypotheses hold, we can conclude that the order of (a, b) is the least common multiple of m and n as required. ■

There is one more result about orders of elements in any group G that will be useful.

Proposition 2.9

If $g \in G$ has order n, then the order of g^m is

$$\frac{l}{m} = \frac{n}{h},$$

where l is the least common multiple of m and n, and h is the highest common factor of m and n. In particular, if m is a factor of n then the order of g^m is $\frac{n}{m}$.

Proof The order of g^m is the least positive integer k such that $g^{mk} = e$. By Exercise 4.7 of Chapter 5, we know that $g^{mk} = e$ precisely when mk is also a multiple of n. So k is the least positive integer such that mk is a multiple of n, hence mk is the least common multiple of m and n. Then $k = \frac{l}{m}$.

Since $mn = hl$ by Proposition 2.6(a), we also have

$$|g^m| = \frac{l}{m} = \frac{n}{h},$$

as required. ■

We can now proceed to consider direct products of cyclic groups. Firstly, we note that, as observed in Subsection 1.2, irrespective of whether the groups are cyclic or not, the order of the direct product of two finite groups is the product of the orders of the individual groups.

Secondly, if the groups concerned are cyclic, then they are abelian, and hence, by Exercise 1.4, so is their direct product.

We can now also use Proposition 2.8 to obtain results of this kind: the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$ is the least common multiple of the order of 1 in $\mathbb{Z}_2$ and the order of 1 in $\mathbb{Z}_3$. Since these orders are 2 and 3, with least common multiple 6, $(1, 1)$ has order 6.

On the other hand, we also know that direct products of cyclic groups are not always cyclic. For example, in Subsection 1.2 we showed that $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and V is not cyclic.

However, sometimes the direct product of cyclic groups *is* cyclic. For example, consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. In Exercise 2.3 we showed that the order of $(1, 1)$ is 6. Since this is the order of $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1, 1) \rangle$, this direct product is indeed cyclic.

So, a direct product of cyclic groups may or may not be cyclic. The aim of this subsection is to determine under what circumstances the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

Exercise 2.5

Show that both of the following direct products are cyclic.

(a) $\mathbb{Z}_3 \times \mathbb{Z}_5$

(b) $\mathbb{Z}_4 \times \mathbb{Z}_5$

In the following exercises you will meet two examples of direct products that are not cyclic even though the factor groups are.

Exercise 2.6

(a) Show that $(1, 1)$ does not generate $\mathbb{Z}_2 \times \mathbb{Z}_4$. Why is this insufficient to prove that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic?

(b) Show that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

In the solution to Exercise 2.6, we saw that the maximum order for an element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ is 4. We could show this directly as follows. If (a, b) is any element of the direct product $\mathbb{Z}_2 \times \mathbb{Z}_4$, then

$$\begin{aligned} 4(a, b) &= (4a, 4b) \\ &= (0, 0). \end{aligned}$$

Exercise 2.7

Show that the order of any element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ is at most 24 and, hence, that this direct product is not cyclic.

Being able to determine the maximum order for any element in a direct product will be useful throughout this chapter, so we generalise the result in Exercises 2.6 and 2.7 in the following proposition.

Proposition 2.10

Let $G = \mathbb{Z}_m \times \mathbb{Z}_n$. Then no element of G can have order greater than the least common multiple of m and n.

Proof Let $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Suppose that a has order r and b has order s. Then by Proposition 4.5 in Chapter 5, we have that r divides m and s divides n. Thus r and s both divide $l = \text{lcm}(m, n)$. Hence

$$l(a, b) = (la, lb) = (e, e).$$

Thus the order of (a, b) is at most l, as required. ■

The property in Proposition 2.10 does not necessarily hold for a direct product where the factor groups are not both cyclic.

Exercise 2.8

Let $G = S_3 \times \mathbb{Z}_3$.

(a) What is m, the maximum order of an element of S_3?

(b) What is n, the maximum order of an element of $\mathbb{Z}_3$?

(c) What is the lowest common multiple of m and n?

(d) Write down an element of order 6 in G.

The following exercise asks you to decide whether some direct products are cyclic.

Exercise 2.9

For each of the following direct products, decide whether or not it is cyclic and justify your conclusion.

(a) $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_9$

Inspecting the examples above suggests that the direct product of cyclic groups *of coprime orders* is cyclic, but if the orders are not coprime then the direct product is not cyclic. This is the content of the next theorem. However, first you are asked to attempt the following exercise, which provides part of the proof of the theorem.

Exercise 2.10

Show that, if m and n are not coprime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Theorem 2.11 *Direct products of cyclic groups*

The direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ of the cyclic groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$ is cyclic if, and only if, m and n are coprime positive integers.

Proof First we prove that, if m and n are coprime, then the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

The element 1 in $\mathbb{Z}_m$ has order m and the element 1 in $\mathbb{Z}_n$ has order n. It follows by Proposition 2.8 that $(1, 1)$ has order $\text{lcm}(m, n)$. By Proposition 2.6, we have that $\text{lcm}(m, n) = mn$. Therefore the order of the element $(1, 1)$ in the direct product is mn. However, the direct product has mn elements and so it is cyclic.

We proved the converse statement in Exercise 2.10, where we showed that if m and n are not coprime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. This is equivalent to showing that if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then m and n are coprime. ■

The next corollary gives an important and useful consequence of Theorem 2.11.

Corollary 2.12

Let m and n be coprime positive integers. Then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Proof We know that the group $\mathbb{Z}_{mn}$ is cyclic and has order mn. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ also has order mn and it is cyclic by Theorem 2.11, we have that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ by Theorem 2.1(b). ■

This corollary is an example of the sort of decomposition result that is our main concern in this book. It leads to the main decomposition theorem for cyclic groups, which we prove later in this subsection.

Exercise 2.11

Show that $\mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

If, in Exercise 2.11, we had decomposed 90 in a different manner, taking $90 = 9 \times 10$, for example, we would have obtained

$$\mathbb{Z}_{90} \cong \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_5.$$

Other decompositions of 90 into a product of pairwise coprime factors produce corresponding direct products. However, Theorem 1.6 ensures that all the resulting direct product decompositions are isomorphic.

Exercise 2.12

Suppose that n is a positive integer with prime decomposition

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers. Show that

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_i = p_i^{k_i}$ for $i = 1, \ldots, r$.

Hint: use induction on r.

The solution to Exercise 2.12 provides a decomposition theorem for finite cyclic groups, which we restate as follows.

Theorem 2.13 *Decomposition of finite cyclic groups*

If n is a positive integer with prime decomposition

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_i = p_i^{k_i}, \quad i = 1, \ldots, r.$

If we combine Theorem 2.13 with the uniqueness of prime decomposition in $\mathbb{Z}$, we see that the decomposition into cyclic groups of prime power order is unique up to isomorphism.

Since each prime power order is a factor of the order of the group, then by Theorem 2.5 each $\mathbb{Z}_{n_i}$ is (isomorphic to) a subgroup. Thus the decomposition theorem expresses the group as a direct product of normal subgroups.

All subgroups of cyclic groups are normal.

We now have a complete description of all cyclic groups, summarised in the three bullet points below.

- Firstly, we have a list of the familiar cyclic groups $\mathbb{Z}$ and $\mathbb{Z}_n$ for each positive n. Every cyclic group is isomorphic to one group in this list.
- Secondly, every finite cyclic group can be written as a direct product in which every factor is a cyclic group of prime power order. These cyclic groups of prime power order cannot be written as direct products of cyclic groups of smaller orders. Thus the cyclic groups of prime power order form a collection of fundamental building blocks from which all finite cyclic groups can be constructed.

The fact that cyclic groups of prime power order cannot be written as direct products of cyclic groups of smaller orders is a consequence of Theorem 2.11.

- Thirdly, we know all about the subgroups of a cyclic group.
  For the infinite cyclic group, $\mathbb{Z}$, the subgroups are precisely the sets $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$, for every non-negative integer n.
  A finite cyclic group has a unique cyclic subgroup corresponding to each factor of its order.

In addition, given any group that is a direct product of cyclic groups, we can factorise it as a direct product of cyclic groups of prime power order.

Exercise 2.13

Prove that the following two groups are isomorphic by factorising each of them as a direct product of cyclic groups of prime power order:

$$\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5 \quad \text{and} \quad \mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}.$$

Exercise 2.14

Factorise the following groups as a direct product of cyclic groups of prime power order.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{75}$

(b) $\mathbb{Z}_9 \times \mathbb{Z}_{21} \times \mathbb{Z}_{245}$

3 Group actions

Each element g of the dihedral group D_4 permutes the positions of vertices of the square. Given a vertex v of the square there is a vertex, which we might denote by $g \wedge v$, to which g sends v. This is an instance of a group *acting* on a set, in this case the set of vertices of the square.

This section formalises the notion of the action of a group on a set, and discusses some specific examples. When we look at a group acting on a set, we hope to gain insight into the symmetry of the set and, at the same time, to obtain a better feel for the group.

This is most obvious when the set is a geometric figure such as the square or circle and the group is its group of symmetries, but there are other significant examples in different contexts. For instance, we will look at the case where $X = \{1, 2, \ldots, n\}$ and G is the symmetric group S_n of all permutations of X, and the case where G is S_4 and X is the set of all polynomials in four variables x_1, x_2, x_3, x_4 with integer coefficients.

3.1 Actions, orbits and stabilisers

The basic idea of a group acting on a set X is that each element of G must send each element of X to another element of X in a way that is compatible with the binary operation in G. This is expressed formally in the following definition.

Definition 3.1 *Group action*

Let G be a group and X a non-empty set. A **group action** of G on X is a function $G \times X \to X$
$(g, x) \mapsto g \wedge x$
that satisfies the following conditions:

(a) $e \wedge x = x$, for all $x \in X$, where e is the identity element of G

(b) $(gh) \wedge x = g \wedge (h \wedge x)$, for all $g, h \in G$ and $x \in X$.

We also say that G **acts** on X by $\wedge$.

Here $(g, x) \mapsto g \wedge x$ simply indicates that the image of the pair (g, x) under the function is denoted by $g \wedge x$.

Note that the definition requires that $g \wedge x$ is an element of X for every $g \in G$ and $x \in X$, so g behaves like a map from X to itself, where the image of $x \in X$ under the map associated with $g \in G$ is $g \wedge x \in X$. The first property in the definition says that the effect of the identity element of G is to leave an element of X unchanged, and the second says that the combined effect of h then g on an element of X is the same as that of the product gh.

We will start by looking at some examples of group actions.

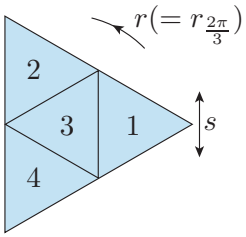


Figure 3.1 Equilateral triangle containing four triangles

Example 3.2 *Action of the group of symmetries on a plane figure*

We divide an equilateral triangle into four smaller triangles numbered $1, 2, 3, 4$ as shown in Figure 3.1.

Let X be the set of triangles $\{1, 2, 3, 4\}$ and let G be the dihedral group D_3, the group of symmetries of an equilateral triangle. Let r be the rotation about the centre of the triangle through $\frac{2\pi}{3}$ and let s be the reflection shown in Figure 3.1. Then

$$D_3 = \{e, r, r^2, s, rs, r^2s\},$$

where rs is the reflection in the line through the centres of triangles 3 and 4, and r^2s is the reflection in the line through the centres of the triangles 2 and 3. Note that $sr = r^2s$.

Then D_3 acts on X using the rule $g \wedge x = g(x)$. It is clear that $g \wedge x$ defined in this way is indeed an element of X. For example, $r \wedge 1 = r(1) = 2$. Therefore $\wedge$ defines a function from $D_3 \times X$ to X.

Below is a complete description of this action.

$e \wedge 1 = 1$	$e \wedge 2 = 2$	$e \wedge 3 = 3$	$e \wedge 4 = 4$
$r \wedge 1 = 2$	$r \wedge 2 = 4$	$r \wedge 3 = 3$	$r \wedge 4 = 1$
$r^2 \wedge 1 = 4$	$r^2 \wedge 2 = 1$	$r^2 \wedge 3 = 3$	$r^2 \wedge 4 = 2$
$s \wedge 1 = 1$	$s \wedge 2 = 4$	$s \wedge 3 = 3$	$s \wedge 4 = 2$
$rs \wedge 1 = 2$	$rs \wedge 2 = 1$	$rs \wedge 3 = 3$	$rs \wedge 4 = 4$
$r^2s \wedge 1 = 4$	$r^2s \wedge 2 = 2$	$r^2s \wedge 3 = 3$	$r^2s \wedge 4 = 1$

Since $e \wedge x = x$, condition (a) in Definition 3.1 is satisfied. Condition (b) holds since $(fg)(x) = (f)(g(x))$ for all $f, g \in D_3$ and $x \in X$.

The next example comes from polynomials in several variables. Group theory partly originated from this type of example.

Example 3.3 *Actions of symmetric groups on sets of polynomials*

Let X be the set of polynomials in three variables and let G be the symmetric group S_3. Let $f \in S_3$ and $p(x_1, x_2, x_3) \in X$. Then we define an action of S_3 on X by

$$f \wedge p(x_1, x_2, x_3) = p(x_{f(1)}, x_{f(2)}, x_{f(3)}).$$

For example, if $f = (1\ 2\ 3)$ and $p = x_1^2x_2 - x_3$ then

$$f \wedge p = x_2^2x_3 - x_1.$$

This example extends to the group S_n acting on the set P_n of polynomials in n variables. We check that this more general example is indeed a group action.

Firstly, $f \wedge p(x_1, x_2, \ldots, x_n) \in P_n$ because of the way $f \wedge p$ has been defined, so $\wedge$ does define a function $S_n \times X \to X$.

Property (a) requires that

$$e \wedge p(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n).$$

This holds because e, the identity of S_n, maps i to i for all $i = 1, \ldots, n$.

Property (b) requires that

$$g \wedge (f \wedge p(x_1, x_2, \ldots, x_n)) = gf \wedge p(x_1, x_2, \ldots, x_n).$$

Now

$$\begin{aligned} g \wedge (f \wedge p(x_1, x_2, \ldots, x_n)) &= g \wedge p(x_{f(1)}, x_{f(2)}, \ldots, x_{f(n)}) \\ &= p(x_{g(f(1))}, x_{g(f(2))}, \ldots, x_{g(f(n))}) \\ &= gf \wedge p(x_1, x_2, \ldots, x_n), \end{aligned}$$

as required. It is worth noticing that this action respects addition and multiplication of polynomials. That is, for all polynomials p and q in $x_1, x_2, \ldots, x_n$,

$$f \wedge (p + q) = f \wedge p + f \wedge q \text{ and } f \wedge (pq) = (f \wedge p)(f \wedge q).$$

For example,

$$(1\,2\,3) \wedge ((x_1 - x_2) + (x_2 - x_3)) = (1\,2\,3) \wedge (x_1 - x_3) = (x_2 - x_1), \quad \text{and}$$
$$(1\,2\,3) \wedge (x_1 - x_2) + (1\,2\,3) \wedge (x_2 - x_3) = (x_2 - x_3) + (x_3 - x_1) = (x_2 - x_1).$$

For an example involving multiplication,

$$\begin{aligned} (1\,2\,3) \wedge (x_1 - x_2)(x_2 - x_3) &= (1\,2\,3) \wedge (x_1x_2 - x_1x_3 - x_2^2 + x_2x_3) \\ &= x_2x_3 - x_2x_1 - x_3^2 + x_3x_1 \\ &= (x_2 - x_3)(x_3 - x_1) \\ &= ((1\,2\,3) \wedge (x_1 - x_2))((1\,2\,3) \wedge (x_2 - x_3)). \end{aligned}$$

Exercise 3.1

Suppose that S_4 acts on the set P_4 of polynomials in four variables in the same way as S_3 acts on the set P_3 of polynomials in three variables as described in Example 3.3. Write down the following.

(a) $(1\,2)(3\,4) \wedge x_1x_2x_3 - x_4$

(b) $(1\,2)(3\,4) \wedge x_1x_2 - x_3x_4$

(c) $(1\,2\,3\,4) \wedge x_1 + x_2 + x_3 + x_4$

Several of our basic examples of groups are groups of functions where the identity is the identity function, that is, a function that leaves every element in the domain fixed.

If X is a non-empty set and G is a group of functions from X to X, then G acts on X by the rule

$$f \wedge x = f(x).$$

We have that $f \wedge x = f(x) \in X$. We check properties (a) and (b) in Definition 3.1:

(a) $e \wedge x = e(x) = x$ for all $x \in X$.

(b) $g \wedge (h \wedge x) = g \wedge h(x) = g(h(x)) = (gh)(x) = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$.

Since both properties are satisfied, we have indeed defined a group action.

The following are examples of this kind of group action.

Example 3.4 *Actions of groups of functions*

1. The symmetric group S_n acts on $\{1, 2, \ldots, n\}$ by the rule $f \wedge x = f(x)$. For example, $(1\,4\,7) \wedge 7 = 1$.
2. The orthogonal group $\mathrm{O}(2, \mathbb{R})$ and the dihedral groups all act on $\mathbb{R}^2$. For example, if r_π denotes rotation through π then
$$r_\pi \wedge (1, 0) = (-1, 0).$$
3. Let X be a geometric figure and let G be its group of symmetries. Then G acts on X with $g \wedge x = g(x)$ for all $g \in G$ and $x \in X$. The rotation group of X also acts on X. For example, the orthogonal group $\mathrm{O}(2, \mathbb{R})$ and the special orthogonal group $\mathrm{SO}(2, \mathbb{R})$ act on the unit circle.

In the next exercise you are asked to prove an elementary consequence of the definition of group action.

Exercise 3.2

Let G be a group acting on a set X by $\wedge$ and let $x \in X$. Let $g \in G$ be such that $g \wedge x = y$. Show that $g^{-1} \wedge y = x$.

In order to prepare for an example of a group action involving the dihedral group D_6, which you met in Exercise 1.6 in Chapter 5, we gather the results of some preliminary calculations in a proposition.

Proposition 3.5

In the group D_6, let r denote a rotation through $\frac{\pi}{3}$ and s denote a reflection in an axis of symmetry, so that
$$r^6 = e, \ s^2 = e \text{ and } sr = r^5 s = r^{-1} s.$$
Then every element of D_6 can be written as $r^m s^n$ for $m = 0, \ldots, 5$ and $n = 0, 1$.

Proof We know that D_6 contains six rotations, each of which has the form $r^m = r^m s^0$ for $m = 0, \ldots, 5$. The other elements of D_6 are six reflections, which have the form $r^m s = r^m s^1$ for $m = 0, \ldots, 5$.

These elements of D_6 are all distinct, since if $r^m s = r^n$ then $r^{m-n} = s$, which is not possible. Thus we have listed all 12 elements of D_6. ■

In the next exercise you can practise manipulating products of elements of D_6. One key trick that is often used in connection with conjugation is to observe that for any elements g and h in a group G,

$$(ghg^{-1})^m = gh^m g^{-1}.$$

This is because $(ghg^{-1})^m = \underbrace{ghg^{-1}ghg^{-1}\cdots ghg^{-1}}_{m \text{ times}}$

$$= g\underbrace{h\cdots h}_{m \text{ times}}g^{-1}$$

$$= gh^m g^{-1}.$$

Exercise 3.3

Consider the group D_6 where r and s are as in Proposition 3.5. Thus

$$r^6 = e,\ s^2 = e \text{ and } sr = r^{-1}s.$$

Show that:

(a) $rs = sr^{-1}$

(b) $srs = r^{-1}$ and $sr^{-1}s = r$

(c) $sr^m s = r^{-m}$ and $sr^{-m}s = r^m$

(d) $sr^m = r^{-m}s$ and $sr^{-m} = r^m s$.

The next example that we want to explore requires some care, not because the idea is harder, but because the set X being acted on is the underlying set of the group doing the acting.

The group in this example is D_6. The set X is the set of elements of D_6. An element g of D_6 acts on an element x of X as follows:

$$g \wedge x = gxg^{-1}.$$

For example, r is an element of D_6 and rs is an element of X, so

$$\begin{aligned} r \wedge (rs) &= r(rs)r^{-1} \\ &= r^2(sr^{-1}) \\ &= r^3 s \qquad \big(\text{since } sr^{-1} = rs \text{ by Exercise 3.3}\big). \end{aligned}$$

This is called the **action of D_6 on itself by conjugation**.

Proposition 3.6

Suppose that the action $\wedge$ by D_6 on the set $X = D_6$ is defined as follows:

$$g \wedge x = gxg^{-1} \text{ for all } g \in D_6 \text{ and } x \in X.$$

Then D_6 acts on X by $\wedge$.

Proof We have that $g \wedge x = gxg^{-1} \in X = D_6$, so $\wedge$ gives a function $D_6 \times D_6 \to D_6$. We check properties (a) and (b) of Definition 3.1.

(a) $e \wedge x = exe^{-1} = exe = x$ for all $x \in X$.

(b) $g \wedge (h \wedge x) = g \wedge hxh^{-1} = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$. ■

In the next exercise you are asked to use the results obtained in Exercise 3.3 to give a complete description of this action. We will then tabulate the results for reference in the later discussion.

Exercise 3.4

Consider the group D_6 where r and s are as in Proposition 3.5 and let D_6 act on itself by conjugation. Show that:

(a) $r^m \wedge r^n = r^n$

(b) $r^m \wedge r^n s = r^{2m+n} s$

(c) $r^m s \wedge r^n = r^{-n}$

(d) $r^m s \wedge r^n s = r^{2m-n} s$.

We now use the fact that $0 \leq m, n \leq 5$ to complete Table 3.1.

Table 3.1 A table showing the action of D_6 on itself by conjugation

$\wedge$	e	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
e	e	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
r	e	r	r^2	r^3	r^4	r^5	r^2s	r^3s	r^4s	r^5s	s	rs
r^2	e	r	r^2	r^3	r^4	r^5	r^4s	r^5s	s	rs	r^2s	r^3s
r^3	e	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
r^4	e	r	r^2	r^3	r^4	r^5	r^2s	r^3s	r^4s	r^5s	s	rs
r^5	e	r	r^2	r^3	r^4	r^5	r^4s	r^5s	s	rs	r^2s	r^3s
s	e	r^5	r^4	r^3	r^2	r	s	r^5s	r^4s	r^3s	r^2s	rs
rs	e	r^5	r^4	r^3	r^2	r	r^2s	rs	s	r^5s	r^4s	r^3s
r^2s	e	r^5	r^4	r^3	r^2	r	r^4s	r^3s	r^2s	rs	s	r^5s
r^3s	e	r^5	r^4	r^3	r^2	r	s	r^5s	r^4s	r^3s	r^2s	rs
r^4s	e	r^5	r^4	r^3	r^2	r	r^2s	rs	s	r^5s	r^4s	r^3s
r^5s	e	r^5	r^4	r^3	r^2	r	r^4s	r^3s	r^2s	rs	s	r^5s

This table illustrates one of the two concepts associated with group actions that we want to discuss here, the concept of an *orbit*. The columns show where each element of $X = D_6$ can be sent under the action by conjugation. Thus r can only be sent to one of r, r^5 and s can only be sent to one of s, r^2s, r^4s.

Definition 3.7 *Orbit*

If a group G acts on a set X and x is an element of X, then the **orbit** of x under G is the set

$$\mathrm{Orb}(x) = \{g \wedge x : \ g \in G\};$$

that is, the set of elements of X obtained by acting on x with the elements of G.

In our first example of a group action – that is, the action of D_3 on four triangles in Example 3.2 – we have

$$\mathrm{Orb}(1) = \{1, 2, 4\} \text{ and } \mathrm{Orb}(3) = \{3\}.$$

Exercise 3.5

Using Table 3.1, determine the orbits of all the elements of D_6 under the action of D_6 defined by $g \wedge x = gxg^{-1}$.

Note the previous exercise shows that there are only six *distinct* orbits in the action of D_6 on itself by conjugation, even though there are 12 elements.

Exercise 3.6

Suppose that S_4 acts on the set P_4 of polynomials in four variables (as in Exercise 3.1). Write down the orbits of:

(a) $x_1x_2x_3 - x_4$

(b) $x_1x_2x_3x_4$

(c) $x_1x_2 + x_3x_4$.

In the solutions to Exercises 3.5 and 3.6, you may have noticed that the orbits partition the set being acted on; that is, the orbits fill out the whole of the set being acted on and do not overlap (unless they coincide). For example, in the action of D_6 on itself by conjugation, the six sets we obtained as orbits were

$$\{e\},\ \{r, r^5\},\ \{r^2, r^4\},\ \{r^3\},\ \{s, r^2s, r^4s\},\ \{rs, r^3s, r^5s\},$$

and these six sets partition D_6.

This is not a coincidence, as the next proposition shows.

Proposition 3.8

Let G be a group acting on a set X. Then the relation $\sim$ on X defined by

$$x \sim y \quad \text{if, and only if, there is } g \in G \text{ such that } x = g \wedge y$$

is an equivalence relation.

Proof For any $x \in X$, we have $e \wedge x = x$, so $\sim$ is a reflexive relation.

Suppose that $x = g \wedge y$ for $x, y \in X$ and $g \in G$. Then, by the solution to Exercise 3.2,

$$y = g^{-1} \wedge x,$$

which shows that $y \sim x$. Thus $\sim$ is symmetric.

If $x, y, z \in X$ are such that $x \sim y$ and $y \sim z$, we have

$$x = g \wedge y \quad \text{and} \quad y = h \wedge z$$

for some $g, h \in G$. Then

$$x = g \wedge (h \wedge z) = gh \wedge z$$

by the definition of group action. It follows that $x \sim z$, therefore $\sim$ is transitive. ■

The equivalence classes of the equivalence relation in Proposition 3.8 are precisely the orbits of the action of G on X. It follows that the orbits give a partition of X.

This fact is useful in proofs about finite groups acting on finite sets, because it tells us that the sum of the sizes of the orbits must be the total number of elements in the set: if

$$\mathrm{Orb}(x_1), \ldots, \mathrm{Orb}(x_n)$$

are the distinct orbits of X under the action of G, then

$$|X| = |\mathrm{Orb}(x_1)| + \cdots + |\mathrm{Orb}(x_n)|\,.$$

Now, the orbit of an element of X is a subset of the set X. The final idea that we want to look at in this chapter concerns certain subsets of the group G, rather than of the set X.

Definition 3.9 *Stabiliser*

If a group G acts on a set X and x is an element of X, then the **stabiliser** of x under G is the set

$$\mathrm{Stab}(x) = \{g : \ g \in G, \ g \wedge x = x\};$$

that is, the set of elements of G that fix x.

In Example 3.2,

$$\mathrm{Stab}(1) = \{e, s\},\ \mathrm{Stab}(2) = \left\{e, r^2 s\right\},\ \mathrm{Stab}(3) = D_3 \ \text{ and } \ \mathrm{Stab}(4) = \{e, rs\}.$$

In the action of D_6 on itself by conjugation, we can see that

$$\mathrm{Stab}(e) = \mathrm{Stab}(r^3) = D_6 \ \text{ and } \ \mathrm{Stab}(r) = \left\{e, r, r^2, r^3, r^4, r^5\right\}.$$

Exercise 3.7

Use Table 3.1 to determine the stabiliser of s under the action of D_6 on itself by conjugation.

You might have observed that all the stabilisers we have found so far are subgroups of the acting group. In the next exercise you are asked to prove that this is no coincidence.

Exercise 3.8

Show that, if G acts on X and $x \in X$, then $\mathrm{Stab}(x)$ is a subgroup of G.

We emphasise an important point about orbits and stabilisers.

If the group G acts on the set X, then:

- orbits are *subsets* of X
- stabilisers are *subgroups* of G.

Exercise 3.9

Suppose that S_3 acts on polynomials in three variables as described in Example 3.3. Write down the stabilisers of:

(a) $x_1x_2^2 + x_2x_3^2 + x_1^2x_3$

(b) $x_1x_2x_3$

(c) x_1x_2.

By now you are familiar with the action of D_6 on itself by conjugation, given by

$$g \wedge x = gxg^{-1}.$$

Any group, not just D_6, acts on itself in this way. The next exercise will show that this action of a group on itself is not the only one possible.

Exercise 3.10

Let $G = S_3$ and define an action of G on $X = S_3$ by

$$g \wedge x = gx.$$

(a) Show that $\wedge$ is a group action.

(b) Write down the orbits of this action.

(c) Write down the stabiliser of $(1\,2\,3)$.

We finish this subsection by stating and proving the Orbit–Stabiliser Theorem that, for a finite group, relates the size of the orbit to that of the stabiliser. First we derive a relationship between $\mathrm{Orb}(x)$ and the left cosets of the stabiliser of x.

Definition 3.10 *$Send_x(y)$*

Let G be a group acting on a set X and let $x \in X$. Then for each element y let

$$\mathrm{Send}_x(y) = \{g \in G : g \wedge x = y\}.$$

So $\mathrm{Send}_x(y)$ is the set of all elements of G that send x to y.

Exercise 3.11

Consider $D_3 = \{e, r, r^2, s, rs, r^2s\}$ and the action described in Example 3.2.

(a) Write down the left cosets of $\mathrm{Stab}(1) = \{e, s\}$.

(b) Write down $\mathrm{Send}_1(1), \mathrm{Send}_1(2)$ and $\mathrm{Send}_1(4)$.

It is no coincidence that the answers to the parts of Exercise 3.11 are the same (see also Example 5.1 of Chapter 5).

Lemma 3.11

Let G be a group acting on a set X, let $x \in X$ and $y \in \mathrm{Orb}(x)$. If $g \in G$ is such that $g \wedge x = y$, then

$$\mathrm{Send}_x(y) = g\mathrm{Stab}(x).$$

Proof Let $h \in \mathrm{Send}_x(y)$ and let $g \wedge x = y$. Then

$$(g^{-1}h) \wedge x = g^{-1} \wedge (h \wedge x) = g^{-1} \wedge y = x$$

by Exercise 3.2. So $g^{-1}h \in \mathrm{Stab}(x)$ and so, since $h = gg^{-1}h$, we have that $h \in g\mathrm{Stab}(x)$. Thus

$$\mathrm{Send}_x(y) \subseteq g\mathrm{Stab}(x).$$

Now suppose that $k \in g\mathrm{Stab}(x)$. Then $k = gh$ for some $h \in \mathrm{Stab}(x)$, and so

$$k \wedge x = (gh) \wedge x = g \wedge (h \wedge x) = g \wedge x = y$$

by definition of g and because $h \in \mathrm{Stab}(x)$. Thus $k \in \mathrm{Send}_x(y)$ and we have shown that

$$g\mathrm{Stab}(x) \subseteq \mathrm{Send}_x(y).$$

Hence $\mathrm{Send}_x(y) = g\mathrm{Stab}(x)$. ■

Lemma 3.11 implies that for each $x \in X$ we can define a function σ_x from $\mathrm{Orb}(x)$ to the set of cosets of $\mathrm{Stab}(x)$. The next theorem shows that this function is a bijection.

Theorem 3.12

Let G be a group acting on a set X, let $x \in X$ and let $H = \mathrm{Stab}(x)$. Let $C(x)$ be the set of left cosets of H in G. Then the function $\sigma_x : \mathrm{Orb}(x) \to C(x)$ defined by

$$\sigma_x : g \wedge x \mapsto gH$$

is a bijection.

Every element of $\mathrm{Orb}(x)$ can be written in the form $g \wedge x$ for some $g \in G$, by definition of $\mathrm{Orb}(x)$.

Proof We need to show that the function σ_x is well defined, one–one and onto.

Suppose that $g \wedge x = h \wedge x = y$. Then g and h both belong to $\mathrm{Send}_x(y)$. By Lemma 3.11, we have

$$\mathrm{Send}_x(y) = gH \quad \text{and} \quad \mathrm{Send}_x(y) = hH,$$

so $\sigma_x(g \wedge x) = gH = hH = \sigma_x(h \wedge x)$, meaning that σ_x is well defined.

To check that σ_x is one–one, pick $g \wedge x$ and $h \wedge x$ in $\mathrm{Orb}(x)$ such that $\sigma_x(g \wedge x) = \sigma_x(h \wedge x)$. Then

$$\begin{aligned} \sigma_x(g \wedge x) = \sigma_x(h \wedge x) &\Rightarrow gH = hH \\ &\Rightarrow h^{-1}g \in H \\ &\Rightarrow h^{-1}g \wedge x = x \quad \text{because } H = \mathrm{Stab}(x) \\ &\Rightarrow g \wedge x = h \wedge x, \end{aligned}$$

which shows that σ_x is one–one.

Finally, any coset gH of H is the image of the element $g \wedge x$ in $\mathrm{Orb}(x)$, which shows that σ_x is onto. ■

It is important to note that, while σ_x in Theorem 3.12 is a bijection, it is not an isomorphism, because the domain $\mathrm{Orb}(x)$ is not a group.

When G is a finite group, Lagrange's Theorem can be combined with Theorem 3.12 to obtain a relationship between the size of the orbit of an element and that of the stabiliser of the same element.

Corollary 3.13 *Orbit–Stabiliser Theorem*

Let G be a finite group acting on the set X. Then, for each $x \in X$,

$$|\mathrm{Orb}(x)| \times |\mathrm{Stab}(x)| = |G|.$$

Proof By Theorem 3.12, the number of elements in $\mathrm{Orb}(x)$ is the same as the number m of left cosets of $\mathrm{Stab}(x)$.

Since the m cosets of $\mathrm{Stab}(x)$ partition G, we have

$$|G| = m\,|\mathrm{Stab}(x)| = |\mathrm{Orb}(x)| \times |\mathrm{Stab}(x)|\,,$$

as required. ■

3.2 Cayley's Theorem

We have seen that several groups, for example the Klein group V, are isomorphic to a subgroup of the symmetric group S_4.

Recall that for any set X, the group of permutations on X (that is, the group of bijections from X to itself with composition of functions) is denoted by S_X. It is reasonable to ask which groups are isomorphic to a subgroup of S_X for some set X. The answer, perhaps surprisingly, is *all* groups.

This was first observed by the mathematician Arthur Cayley and we state this result as a theorem bearing his name.

We will prove Cayley's Theorem using an action of a group G on itself called the **action by left multiplication**. You met a special case of this action in Exercise 3.10. It is defined by

$$g \wedge x = gx \quad \text{for all} \quad g, x \in G.$$

We check that this definition gives indeed an action of G on itself using exactly the same method as in Exercise 3.10. First of all,

$$g \wedge x = gx \in X = G.$$

Moreover:

(a) $e \wedge x = ex = x$ for all $x \in X$

(b) $g \wedge (h \wedge x) = g \wedge (hx) = (gh)x = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$.

So, by Definition 3.1, G acts on itself by $\wedge$.

Before stating and proving Cayley's Theorem, we give an example that illustrates the method of proof.

Example 3.14 *An action by left multiplication*

Let $G = \{e, r, h, v\}$ be the group of symmetries of the rectangle and consider the action of G on itself by left multiplication. Number the elements of G as follows:

$$e = g_1, \quad r = g_2, \quad h = g_3 \quad \text{and} \quad v = g_4.$$

Now consider the action of r on each element of G:

$$r \wedge g_1 = rg_1 = g_2, \quad r \wedge g_2 = g_1, \quad r \wedge g_3 = g_4 \quad \text{and} \quad r \wedge g_4 = g_3.$$

Thus, the action of r swaps g_1 and g_2, and it also swaps g_3 and g_4. In fact, one way to describe this action is via a permutation f_r of G, namely

$$(g_1\, g_2)(g_3\, g_4).$$

Once we have numbered the elements of G, there is no ambiguity in denoting f_r via the indices of the elements it permutes, that is, via the permutation $(1\,2)(3\,4)$.

We can obtain a permutation representation for all the other elements of G in this way, and we get

$$f_e = e, \quad f_h = (1\,3)(2\,4) \quad \text{and} \quad f_v = (1\,4)(2\,3).$$

In fact, we can define a homomorphism $f : G \to S_4$ by

$$f : g \mapsto f_g.$$

This homomorphism is injective and the image

$$f(G) = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

is isomorphic to the Klein group.

Theorem 3.15 *Cayley's Theorem*

Every group G is isomorphic to a subgroup of S_G, the group of permutations of G.

In particular, if G is finite then G is isomorphic to a subgroup of S_n, where $n = |G|$.

Proof Let G act on itself by left multiplication, that is, by

$$g \wedge x = gx \text{ for all } g, x \in G.$$

Define a map $\phi : G \to S_G$, so that, for $g \in G$, $\phi(g) = \phi_g$ is the permutation of G given by

$$\phi_g(x) = g \wedge x = gx.$$

Then for g, h and x in G,

$$\phi_{gh}(x) = gh \wedge x = g \wedge (h \wedge x) = \phi_g \phi_h(x),$$

so ϕ is a homomorphism. This homomorphism is injective, for if $\phi_g = \phi_h$ then

$$g = ge = \phi_g(e) = \phi_h(e) = he = h.$$

Hence G is isomorphic to its image $\phi(G)$, which is a subgroup of S_G.

If G is finite and of order n then, as in Example 3.14, we identify S_G with S_n by numbering the elements of G from 1 to n. ■

Exercise 3.12

Use the approach given in the proof of Cayley's Theorem to find a subgroup of S_8 that is isomorphic to $G = \mathbb{Z}_4 \times \mathbb{Z}_2$.

Note that the homomorphism you found in Exercise 3.12 is by no means the only homomorphism between $\mathbb{Z}_4 \times \mathbb{Z}_2$ and a subgroup of a finite permutation group. Indeed, there may be simpler homomorphisms, and ones where the codomain is a subgroup of some S_n for $n \neq 8$. For example, we can construct a homomorphism from G to S_6 with

$(1, 0) \mapsto (1\,2\,3\,4)$ and
$(0, 1) \mapsto (5\,6)$.

3.3 Cauchy's Theorem

We now aim to prove that for any prime number p, every finite group G whose order is a multiple of p must contain an element of order p. This result is called Cauchy's Theorem. In order to prove Cauchy's Theorem, we work with a specific group action, and before we look at the general description of this action, we consider a particular example.

By now you should be quite familiar with the dihedral group

$$D_3 = \{e, r, r^2, s, rs, r^2 s\},$$

the group of symmetries of an equilateral triangle. The element r is the rotation about the centre of the triangle through $\frac{2\pi}{3}$, and s is the reflection shown in Figure 3.2. The elements rs and $r^2 s$ then give the other two reflections. Remember that

$$sr = r^2 s \quad \text{and} \quad sr^2 = rs.$$

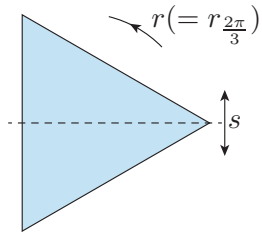


Figure 3.2 Symmetries of an equilateral triangle

There is an action of the group S_3 on the set Y of all triples (g_1, g_2, g_3) of elements of D_3 that works as follows. For $a \in S_3$, the action applies the permutation $a \in S_3$ to each component of the triple. For example,

$$(1\,2\,3) \wedge (r, r^2, e) = (e, r, r^2) \quad \text{and}$$
$$(1\,2) \wedge (r, r^2, e) = (r^2, r, e).$$

The requirements for an action are clearly satisfied – the second requirement follows from the fact that composition of functions is associative.

Now let $A = \langle (1\,2\,3) \rangle$ be the cyclic subgroup of S_3 generated by $(1\,2\,3)$ and let X be the set of triples (g_1, g_2, g_3), where each $g_i \in D_3$ and $g_1 g_2 g_3 = e$. Examples of elements of X are (r, r^2, e), (s, e, s) and, since r^2 has order 3, also (r^2, r^2, r^2). Notice that in each case we have $g_3 = (g_1 g_2)^{-1}$, which is equivalent to $g_1 g_2 g_3 = e$.

Now let $x = (g_1, g_2, g_3)$ be an element of X, so $g_1 g_2 g_3 = e$. The three elements of A act on x as follows:

$$e \wedge x = x, \quad (1\,2\,3) \wedge x = (g_3, g_1, g_2), \quad (1\,3\,2) \wedge x = (g_2, g_3, g_1).$$

We have

$$g_3 g_1 g_2 = (g_1 g_2)^{-1} g_1 g_2 = e \quad \text{and}$$
$$g_2 g_3 g_1 = g_2 (g_1 g_2)^{-1} g_1 = g_2 g_2^{-1} g_1^{-1} g_1 = e,$$

so $a \wedge x \in X$ for all $x \in X$ and all $a \in A$.

Thus we have indeed defined an action of the subgroup A on the set X.

How big is the set X? There are six independent choices for each of the first two elements g_1, g_2 of (g_1, g_2, g_3), since $|D_3| = 6$, but g_3 is then determined and must be $(g_1 g_2)^{-1}$. Therefore

$$|X| = 6 \times 6 = 36.$$

The next exercise is intended to help you understand the key points of the proof of Cauchy's Theorem, which follows it.

Exercise 3.13

Consider the action of A on X described above.

(a) Find $g_3 \in D_3$ such that $(r, s, g_3) \in X$. How many elements of X are in the orbit of (r, s, g_3)?

(b) Find $g_3 \in D_3$ such that $(r, r, g_3) \in X$. How many elements of X are in the orbit of (r, r, g_3)?

(c) Which elements (g_1, g_2, g_3) of X are stabilised by $(1\,2\,3)$?

Theorem 3.16 *Cauchy's Theorem*

Let G be a group of order n and let p be a prime divisor of n. Then G has an element of order p.

Proof Let A be the cyclic subgroup of S_p generated by $(1\,2\,\ldots\,p)$ and let X be the set of p-tuples $(g_1, g_2, \ldots, g_p)$ where each g_i is an element of G and

$$g_1 g_2 \cdots g_p = e.$$

Let $a \in A$ and let $x = (g_1, g_2, \ldots, g_p) \in X$. We check that $a \wedge x \in X$, where $\wedge$ is the action described above.

Now $g_p = (g_1 \cdots g_{p-1})^{-1}$, so $x = (g_1, \ldots, g_{p-1}, (g_1 g_2 \cdots g_{p-1})^{-1})$.

Then $a \wedge x$ is obtained from x by cyclically permuting the g_is, so

$$a \wedge x = (g_i, \ldots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}, g_1, \ldots, g_{i-1}) \text{ where } a(i) = 1.$$

Now

$$\begin{aligned} &g_i \cdots g_{p-1}(g_1 \cdots g_{p-1})^{-1} g_1 \cdots g_{i-1} \\ &\quad = (g_i \cdots g_{p-1} g_{p-1}^{-1} \cdots g_i^{-1})(g_{i-1}^{-1} \cdots g_1^{-1} g_1 \cdots g_{i-1}) \\ &\quad = e, \end{aligned}$$

and so $a \wedge x \in X$ as required. Hence A acts on X by $\wedge$.

Since A has prime order p, we know from Corollary 3.13 that each orbit of this action of A must have either p elements or 1 element. Let s be the number of orbits with p elements and t be the number of orbits with one element. The orbits partition X so X has precisely $ps + t$ elements.

We can count the number of elements in X in another way. For each of $g_1, g_2, \ldots, g_{p-1}$ we have n independent choices of elements of G, but then g_p is determined by $g_p = (g_1 \cdots g_{p-1})^{-1}$.

Thus X has n^{p-1} elements. As p is a factor of n, we have that $n = pm$ for some integer m.

Hence $ps + t = |X| = n^{p-1} = (pm)^{p-1}$, and so

$$t = (pm)^{p-1} - ps = pq, \qquad \text{where } q = (p^{p-2}m^{p-1} - s).$$

Now $t > 0$, because the orbit of $(e, e, \ldots, e)$ has only one element. As $t = pq$ is a positive multiple of p it follows that $t \geq p > 1$.

We now know that, apart from $(e, e, \ldots, e)$, there is at least one other element $x = (g_1, g_2, \ldots, g_p)$ whose orbit has only one element. Such an element x is stabilised by $(1\,2\,\ldots\,p)$, so we must have $g_1 = g_2 = \cdots = g_p = g$, say, and $x = (g, g, \ldots, g)$. We have that $g^p = e$ because $x \in X$, and $g \neq e$ because $x \neq (e, e, \ldots, e)$.

By Exercise 4.7 of Chapter 5, the order of g must be a divisor of p. Since p is prime and g cannot have order 1, the order of g must be p. ■

Exercise 3.14

Let G be a group of order 6.

(a) Show that G has a cyclic subgroup of order 3 and a cyclic subgroup of order 2.

(b) Suppose that G is abelian. Let $a \in G$ have order 3 and $b \in G$ have order 2. What is the order of ab? Show that G is cyclic.

3.4 Finite abelian groups

We finish this chapter by proving some results that take us a further step along the way to classifying finite abelian groups.

Theorem 3.17

Let G be a finite abelian group of order n, where

$$n = p_1 p_2 \cdots p_r$$

for r distinct primes $p_1, p_2, \ldots, p_r$. Then G is cyclic and of order n. Moreover,

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_r}.$$

Proof By Cauchy's Theorem, G has r cyclic subgroups $\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_r}$.

For each i in $\{1, \ldots, r\}$, let g_i be a generator for $\mathbb{Z}_{p_i}$ so that g_i has order p_i. In fact, any non-identity element of $\mathbb{Z}_{p_i}$ generates the group.

Since $p_1, \ldots, p_r$ are distinct primes, the element $g_1 g_2 \cdots g_r$ has order

$$p_1 p_2 \cdots p_r = n$$

by the solution of Exercise 2.4. Thus G is cyclic and generated by this element.

It follows from Theorem 2.13 that $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_r}$, as required. ■

Theorem 3.17 applies to the rather special case of abelian groups whose order is a product of prime numbers. There is a result of the same flavour for abelian groups whose order is a *power* of a prime. This result requires a lemma whose proof is slightly technical and which uses additive notation for improved readability. The proof also makes use of Exercise 1.10.

In additive notation, Exercise 1.10 shows that if G is an abelian group and H_1, H_2 are subgroups of G with $H_1 \cap H_2 = \{0\}$, then whenever $h_1 \in H_1$ and $h_2 \in H_2$ are such that

$$h_1 + h_2 = 0,$$

then $h_1 = 0$ and $h_2 = 0$.

We pull out a small part of the proof of Lemma 3.18 below as an exercise.

Exercise 3.15

Suppose that G is an abelian group, written in additive notation, and let A be a subgroup of G. Suppose that $y \in G$, and $py, dy \in A$, where p and d are coprime integers. Show that $y \in A$.

Lemma 3.18

Suppose that G is an abelian group of order p^n for some prime p and some positive integer n. Then

$$G \cong H \times K,$$

where H is a cyclic subgroup of G of order p^r, for some positive integer r.

Proof By Proposition 4.5 of Chapter 5, the order of any element of G divides p^n. Choose $g \in G$ such that g has order p^r, where p^r is maximal among the orders of elements of G.

Let $H = \langle g \rangle$ be the cyclic subgroup generated by g. The maximality of p^r means that $p^r x = 0$ for all $x \in G$.

Consider the set of all subgroups of G whose intersection with H is $\{0\}$. This set is non-empty since it contains the trivial subgroup. Let K be maximal in this set. Then $H \cap K = \{0\}$, but for any proper subgroup K' of G such that $K \leq K'$ and $K' \neq K$ the maximality of K implies that $H \cap K' \neq \{0\}$.

K' is a *proper* subgroup of G if $K' \leq G$ and $K' \neq G$.

We aim to show that $G = H \times K$. By way of contradiction, let $x \in G \setminus (H \times K)$. Now

$$p^r x = 0 \in H \times K,$$

Recall that the notation $A \setminus B$, sometimes written $A - B$, denotes the set A excluding any elements of B.

so we can choose $m \leq r$ such that $p^m x \in H \times K$ but $p^{m-1}x \notin H \times K$ (if no such m existed, we would have $p^{m-1}x \in H \times K$ for all $m \in \{1, \ldots, r\}$, including $p^0 x = x$, contradicting our choice of x).

Let $y = p^{m-1}x$. Then, since $py \in H \times K$, we can write $py = ag + k$ for some $a \in \mathbb{Z}$ and $k \in K$.

From our choice of r, we have that

$$0 = p^r y = p^{r-1}(ag + k) = p^{r-1}ag + p^{r-1}k.$$

We started with an element y with $py \in H \times K$ but $y \notin H \times K$, and from this we have constructed an element $z = y - bg$ with $pz \in K$ but $z \notin K$.

Since $H \cap K = \{0\}$, by Exercise 1.10 this means that $p^{r-1}ag = 0$, and so p divides a. Thus we can write $py = pbg + k$ for some integer b, and so $p(y - bg) \in K$. Consider the element $y - bg$. Now, if $y - bg \in K$ then $y = bg + k_1$ for some $k_1 \in K$, which gives $y \in H \times K$. Since $y \notin H \times K$, we must have $y - bg \notin K$.

Let $K' = \langle K, y - bg \rangle$, the subgroup generated by K and $y - bg$. Then $K' \neq K$. By our choice of K, we have $K' \cap H \neq \{0\}$. Thus there exists $c \in \mathbb{Z}$ with $c \neq 0$ and

$$cg = k + d(y - bg).$$

Now p does not divide d, because $H \cap K = \{0\}$ and $p(y - bg) \in K$. Thus $\mathrm{hcf}(p, d) = 1$.

But now we have

$$dy = cg + dbg - k \in H \times K \quad \text{and} \quad py \in H \times K.$$

Thus, since $\mathrm{hcf}(p, d) = 1$, by Exercise 3.15 we have $y \in H \times K$, which is a contradiction.

This means that there can be no $x \in G \setminus H \times K$. So we have $G = H \times K$, as required. ■

Lemma 3.18 enables us to prove that every abelian group whose order is the power of a prime is a direct product of cyclic groups.

Theorem 3.19

Let G be an abelian group of order p^n for some positive integer n and for some prime p. Then G is a direct product of cyclic subgroups.

Proof We prove this result by induction on n.

Firstly, the result is true for $n = 1$, since in that case

$$G \cong \mathbb{Z}_p \, (\cong \mathbb{Z}_p \times \{0\}).$$

Now suppose that the result holds for all abelian groups of order p^m with $m < n$, and suppose that G has order p^n.

By Lemma 3.18, we know $G \cong H \times K$ where H is a non-trivial cyclic subgroup of G. Thus $|K|$ is p^m for some $m < n$, and we can use the induction hypothesis that K is a direct product of cyclic subgroups of K to conclude that G is a direct product of cyclic subgroups, as required. ■

Exercise 3.16

Let G be an abelian group of order 8. Write down all the possible groups to which G might be isomorphic.

We need just a little more machinery before we can prove that all finite abelian groups are direct products of cyclic groups. This result, which will be proved in Chapter 8, Subsection 2.1, will be one of the main results in this book.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Apply the Internal Direct Product Theorem in simple cases.

(b) Decide whether a given group is cyclic.

(c) Given a finite cyclic group, find a generator for a subgroup of a given order.

(d) Express a given finite cyclic group as the direct product of cyclic groups of prime power order.

(e) Given two direct products of cyclic groups, determine whether or not they are isomorphic.

(f) For a group G and a set X, check whether a given function $G \times X \to X$ is a group action.

(g) Identify the orbit of an element of a set X acted on by a group G.

(h) Identify the stabiliser of an element of a set X acted on by a group G.

(i) Apply Cauchy's Theorem to show the existence of certain subgroups of prime order.

(j) Work with the action used in the proof of Cauchy's Theorem in specific examples of groups.

(k) Prove simple results about abelian groups, cyclic groups and direct products.

Solutions to exercises

Solution to Exercise 1.1

Closure Let (x_1, y_1) and (x_2, y_2) be any two elements of $\mathbb{R} \times \mathbb{R}$. By definition, x_1, y_1, x_2 and y_2 are in $\mathbb{R}$. Since $\mathbb{R}$ is closed under addition, it follows that $x_1 + x_2$ and $y_1 + y_2$ are also in $\mathbb{R}$. By definition,

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

so, by the above, this sum is an element of $\mathbb{R} \times \mathbb{R}$. Therefore the operation $+$ satisfies the closure axiom.

Associativity Let (x_1, y_1), (x_2, y_2) and (x_3, y_3) be three elements of $\mathbb{R} \times \mathbb{R}$. By definition,

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \text{ and}$$
$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1 + (x_2 + x_3),\ y_1 + (y_2 + y_3)).$$

The right-hand sides of these two equations are equal, since addition in $\mathbb{R}$ is associative. Hence

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1, y_1) + ((x_2, y_2) + (x_3, y_3))$$

and so $+$ in $\mathbb{R} \times \mathbb{R}$ is associative.

Identity The element $(0, 0)$ belongs to $\mathbb{R} \times \mathbb{R}$, and

$$(0, 0) + (x, y) = (x, y) + (0, 0) = (x, y)$$

for any (x, y) in $\mathbb{R} \times \mathbb{R}$. Therefore $(0, 0)$ is the identity of $\mathbb{R} \times \mathbb{R}$, and the identity axiom is satisfied.

Inverses If (x, y) is any element of $\mathbb{R} \times \mathbb{R}$ then, as x and y are in $\mathbb{R}$, their additive inverses $-x$ and $-y$ are also in $\mathbb{R}$. So the element $(-x, -y)$ is an element of $\mathbb{R} \times \mathbb{R}$. Furthermore,

$$(x, y) + (-x, -y) = (0, 0) = (-x, -y) + (x, y).$$

So $(-x, -y)$ is the inverse of the element (x, y), and the inverses axiom is satisfied.

Solution to Exercise 1.2

The underlying set is

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_3 &= \{0, 1\} \times \{0, 1, 2\} \\ &= \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}. \end{aligned}$$

The Cayley table is constructed using addition modulo 2 for the first components and addition modulo 3 for the second.

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Solution to Exercise 1.3

(a) Let (g_1, h_1), (g_2, h_2) and (g_3, h_3) be any three elements of $G \times H$. Then

$$\begin{aligned}
&((g_1, h_1) \bullet (g_2, h_2)) \bullet (g_3, h_3) \\
&\quad = (g_1 \circ g_2, h_1 * h_2) \bullet (g_3, h_3) && \text{by the definition of } \bullet \\
&\quad = ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) && \text{by the definition of } \bullet \\
&\quad = (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) && \text{by the associativity axiom for } G \text{ and } H \\
&\quad = (g_1, h_1) \bullet ((g_2 \circ g_3), (h_2 * h_3)) && \text{by the definition of } \bullet \\
&\quad = (g_1, h_1) \bullet ((g_2, h_2) \bullet (g_3, h_3)) && \text{by the definition of } \bullet .
\end{aligned}$$

(b) Let (g, h) be any element of the direct product $G \times H$. Then

$$\begin{aligned}
(e_G, e_H) \bullet (g, h) &= (e_G \circ g, e_H * h) && \text{by the definition of } \bullet \\
&= (g, h) && \text{by the identity axiom for } G \text{ and } H.
\end{aligned}$$

Similarly,

$$(g, h) \bullet (e_G, e_H) = (g, h).$$

Hence (e_G, e_H) is the identity element of the direct product.

(c) Applying the inverse properties for the groups G and H, we have

$$\begin{aligned}
(g, h) \bullet (g^{-1}, h^{-1}) &= (g \circ g^{-1}, h * h^{-1}) && \text{by the definition of } \bullet \\
&= (e_G, e_H) && \text{by the inverses axiom for } G \text{ and } H.
\end{aligned}$$

Similarly,

$$(g^{-1}, h^{-1}) \bullet (g, h) = (e_G, e_H).$$

Hence (g^{-1}, h^{-1}) is the inverse of (g, h).

Solution to Exercise 1.4

Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then

$$\begin{aligned}
(g_1, h_1)(g_2, h_2) &= (g_1 g_2, h_1 h_2) \\
&= (g_2 g_1, h_2 h_1)
\end{aligned}$$

since G and H are both abelian. But

$$(g_2 g_1, h_2 h_1) = (g_2, h_2)(g_1, h_1),$$

so the direct product $G \times H$ is abelian.

Solution to Exercise 1.5

Assume that $h \in H_1 \cap H_2$. We can express h in two ways as an element of H_1H_2, namely

$$h = he, \text{ with } h \in H_1,\ e \in H_2, \text{ and}$$
$$h = eh, \text{ with } e \in H_1,\ h \in H_2.$$

Hence $\phi(h, e) = \phi(e, h)$, and, since ϕ is one–one, we have

$$(h, e) = (e, h).$$

Then $h = e$ by the definition of an ordered pair. Thus the only element in $H_1 \cap H_2$ is the identity, as required.

Solution to Exercise 1.6

As before, we write $a = h_1h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.

Let aha^{-1} be any element of aH_2a^{-1}, where $h \in H_2$. Then

$$\begin{aligned} aha^{-1} &= (h_1h_2)h(h_1h_2)^{-1} \\ &= h_1h_2hh_2^{-1}h_1^{-1} \\ &= h_1(h_2hh_2^{-1})h_1^{-1} \\ &= h_1h'h_1^{-1} \qquad (\text{where } h' = h_2hh_2^{-1} \in H_2) \\ &= h'h_1h_1^{-1} \qquad (\text{since } h_1 \in H_1 \text{ and } h' \in H_2 \text{ commute}) \\ &= h' \in H_2, \end{aligned}$$

and so $aH_2a^{-1} \subseteq H_2$.

Solution to Exercise 1.7

We can define the subgroups as follows:

$$H_1 = \langle a^3 \rangle = \{e, a^3\},$$
$$H_2 = \langle a^2 \rangle = \{e, a^2, a^4\}.$$

Note that $H_1 \cong \mathbb{Z}_2$ and $H_2 \cong \mathbb{Z}_3$.

Since e, a^2, a^3, a^4, a^5 are all in H_1H_2 and

$$a^3a^4 = a^7 = a,$$

we see that $\mathbb{Z}_6 = H_1H_2$.

Next, by inspection, $H_1 \cap H_2 = \{e\}$.

Lastly, we must check that H_1 and H_2 are both normal in $\mathbb{Z}_6$. But $\mathbb{Z}_6$ is abelian, so every subgroup is normal.

Hence H_1 and H_2 satisfy the conditions in Theorem 1.5, and we can conclude that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, as required.

Solution to Exercise 1.8

Let $g = h^{-1}k^{-1}hk$. Since K is a normal subgroup of $G, h^{-1}k^{-1}h \in K$; and so, since $k \in K, g \in K$. Since H is a normal subgroup of G, $k^{-1}hk \in H$; and so, since $h \in H, g \in H$. Thus $g \in H \cap K = \{e\}$ and so $g = e$. That is, $h^{-1}k^{-1}hk = e$, and so by multiplying on the left by kh we see that $hk = kh$.

Solution to Exercise 1.9

Suppose that $\psi(a_1, (b_1, c_1)) = \psi(a_2, (b_2, c_2))$. By the definition of ψ,

$$((a_1, b_1), c_1) = ((a_2, b_2), c_2).$$

By the definition of ordered pairs, $(a_1, b_1) = (a_2, b_2)$ and $c_1 = c_2$. Applying the definition of ordered pairs again, we get $a_1 = a_2$ and $b_1 = b_2$. Hence $(a_1, (b_1, c_1)) = (a_2, (b_2, c_2))$. This shows that ψ is one–one.

To see that ψ is onto, let $((a, b), c)$ be any element of the codomain. Then $a \in A, b \in B, c \in C$, and so $(a, (b, c)) \in A \times (B \times C)$ and $\psi(a, (b, c)) = ((a, b), c)$. Hence ψ is onto.

To check the morphism property, let $(a_1, (b_1, c_1))$ and $(a_2, (b_2, c_2))$ be any two elements of the domain. Then

$$\begin{aligned}
\psi((a_1, (b_1, c_1))(a_2, (b_2, c_2))) &= \psi(a_1a_2, ((b_1, c_1)(b_2, c_2))) \\
&= \psi(a_1a_2, (b_1b_2, c_1c_2)) \\
&= ((a_1a_2, b_1b_2), c_1c_2) \\
&= ((a_1, b_1)(a_2, b_2), c_1c_2) \\
&= ((a_1, b_1), c_1)((a_2, b_2), c_2) \\
&= \psi(a_1, (b_1, c_1))\psi((a_2, (b_2, c_2)).
\end{aligned}$$

This completes the proof that ψ is an isomorphism.

Solution to Exercise 1.10

Since G is abelian, the elements of H_1 and H_2 commute, so we can apply Proposition 1.9(b) to conclude that $H_1H_2 \cong H_1 \times H_2$ via the isomorphism $\psi : H_1H_2 \to H_1 \times H_2$ defined by

$$x_1x_2 \mapsto (x_1, x_2).$$

If $h_1h_2 = 1$, then $(h_1, h_2) = \psi(h_1h_2) = \psi(1)$. Since ψ must map the identity in H_1H_2 to the identity in $H_1 \times H_2$, we must have $(h_1, h_2) = (1, 1)$, which gives the required result.

Solution to Exercise 2.1

(a) Since m is the least positive exponent such that a^m is in H, we have $k \geq m$ and we can use the Division Algorithm (Book A, Chapter 1, Theorem 4.1) to write $k = mq + r$ where $0 \leq r < m$. Hence $r = k - mq$, and so

$$\begin{aligned}
a^r &= a^{k-mq} \\
&= a^k a^{-mq} \\
&= a^k (a^m)^{-q}.
\end{aligned}$$

Since a^k and a^m belong to H, so does a^r.

Now, m was chosen as the least *positive* exponent appearing in H, so we must have $r = 0$, and hence $m \mid k$. We have shown that every element a^k of H is a power $a^k = a^{mq} = (a^m)^q$ of a^m, which completes the proof that $H = \langle a^m \rangle$.

(b) Since $a^n = e$, which is an element of H, from part (a) we have that $m \mid n$.

(c) Let $n = mq$. We first observe that $e = a^n = a^{mq} = (a^m)^q$. So q is a positive power of a^m that produces the identity. It remains to prove that q is the smallest such power of a^m.

Consider a positive power k of a^m that is the identity; that is, $e = (a^m)^k = a^{mk}$. Since the order of a is n, this can only be true if $mk \geq n = mq$. Hence $k \geq q$. Therefore q is the least power of a^m that gives the identity. Hence the order of a^m, and therefore the order of H, is q.

Solution to Exercise 2.2

(a) The divisors of 24 are $1, 2, 3, 4, 6, 8, 12$ and 24, so $\mathbb{Z}_{24}$ will have a subgroup of each of these orders.

(b) (i) The subgroups are isomorphic to $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$ and $\mathbb{Z}_{24}$, respectively.

(ii) The first subgroup in the list is the trivial subgroup, generated by $\frac{24}{1} \equiv 0 \pmod{24}$.

The remaining ones have generators $12, 8, 6, 4, 3, 2$ and 1, respectively.

We list the generators, the elements generated and the cyclic group to which the subgroup is isomorphic in the table below.

Generator (mod 24)	Elements generated	Isomorphic group
$\frac{24}{1} \equiv 0$	$\{0\}$	$\mathbb{Z}_1$
$\frac{24}{2} \equiv 12$	$\{0, 12\}$	$\mathbb{Z}_2$
$\frac{24}{3} \equiv 8$	$\{0, 8, 16\}$	$\mathbb{Z}_3$
$\frac{24}{4} \equiv 6$	$\{0, 6, 12, 18\}$	$\mathbb{Z}_4$
$\frac{24}{6} \equiv 4$	$\{0, 4, 8, 12, 16, 20\}$	$\mathbb{Z}_6$
$\frac{24}{8} \equiv 3$	$\{0, 3, 6, 9, 12, 15, 18, 21\}$	$\mathbb{Z}_8$
$\frac{24}{12} \equiv 2$	$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$	$\mathbb{Z}_{12}$
$\frac{24}{24} \equiv 1$	$\{0, 1, \ldots, 23\}$	$\mathbb{Z}_{24}$

Solution to Exercise 2.3

We use additive notation so that $(0,0)$ denotes the identity in both cases, and we write $n(x,y)$ for $\underbrace{(x,y)+\cdots+(x,y)}_{n \text{ times}}$.

(a) We have $(1,1) = (1,1)$, $2(1,1) = (0,2)$, $3(1,1) = (1,0)$,
$4(1,1) = (0,1)$, $5(1,1) = (1,2)$, $6(1,1) = (0,0)$.
Hence $(1,1)$ has order 6.

(b) We have $1(1,1) = (1,1)$ and $2(1,1) = (0,0)$. Hence $(1,1)$ has order 2.

Solution to Exercise 2.4

We use induction on r, the number of elements in the product. For $r = 2$, the result follows from Lemma 2.7, since G is abelian and p_1 and p_2 are distinct primes, so that $\langle g_1\rangle \cap \langle g_2\rangle = \{e\}$.

Suppose the result is true for $r = k$; that is, if $g_1, g_2, \ldots, g_k$ are elements of G that have distinct prime order $p_1, p_2, \ldots, p_r$ respectively, then the order of $g_1 g_2 \cdots g_k$ is $p_1 p_2 \cdots p_k$.

Let g_{k+1} be an element of G of order p_{k+1}, where p_{k+1} is prime and distinct from $p_1, p_2, \ldots, p_k$. Then

$$\langle g_1 g_2 \cdots g_k\rangle \cap \langle g_{k+1}\rangle = \{e\}$$

since no elements of $\langle g_1 g_2 \cdots g_k\rangle$ can have order p_{k+1}, and so we can apply Lemma 2.7 to obtain that the order of $g_1 g_2 \cdots g_{k+1}$ is $p_1 p_2 \cdots p_{k+1}$.

The result follows by induction.

Solution to Exercise 2.5

By Proposition 2.8, the order of the element $(1,1)$ in the direct product is the least common multiple of the orders of the element 1 in each of the factor groups.

(a) The order of 1 in $\mathbb{Z}_3$ is 3 and the order of 1 in $\mathbb{Z}_5$ is 5.
Since $\operatorname{lcm}(3,5) = 15$, the element $(1,1)$ has order 15 in $\mathbb{Z}_3 \times \mathbb{Z}_5$.
As $\mathbb{Z}_3 \times \mathbb{Z}_5$ has 15 elements, it is cyclic.

(b) The order of 1 in $\mathbb{Z}_4$ is 4 and the order of 1 in $\mathbb{Z}_5$ is 5.
Since $\operatorname{lcm}(4,5) = 20$, the element $(1,1)$ has order 20 in $\mathbb{Z}_4 \times \mathbb{Z}_5$.
As $\mathbb{Z}_4 \times \mathbb{Z}_5$ has 20 elements, it is cyclic.

Solution to Exercise 2.6

(a) The order of 1 in $\mathbb{Z}_2$ is 2 and the order of 1 in $\mathbb{Z}_4$ is 4.
Since $\operatorname{lcm}(2,4) = 4$, the element $(1,1)$ has order 4 in $\mathbb{Z}_2 \times \mathbb{Z}_4$.
As $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 8 elements, it is not generated by $(1,1)$.

All we have done is to show that $(1,1)$ is not a generator. To show that the direct product is not cyclic, we would have to show that *none* of the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ generates the whole group.

(b) If (a, b) is any element of $\mathbb{Z}_2 \times \mathbb{Z}_4$, then a has order 1 or 2 and b has order 1, 2 or 4. The only possible least common multiples of the orders of a and b are 1, 2 and 4. Hence no element of the direct product has order 8, and so $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

Solution to Exercise 2.7

Let $a \in \mathbb{Z}_6$. Then $6a = 0$. Similarly, if $b \in \mathbb{Z}_8$, then $8b = 0$. Hence for any element (a, b) in $\mathbb{Z}_6 \times \mathbb{Z}_8$, we have

$$\begin{aligned} 24(a, b) &= (24a, 24b) \\ &= (4(6a), 3(8b)) \\ &= (0, 0). \end{aligned}$$

So the maximum order of any element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ is at most 24. Since this direct product has order 48, it cannot be cyclic.

Solution to Exercise 2.8

(a) The maximum order of an element of S_3 is 3.

(b) The maximum order of an element of $\mathbb{Z}_3$ is 3.

(c) The lowest common multiple is 3.

(d) $((1\,2), 1)$ has order 6.

Solution to Exercise 2.9

(a) The group $\mathbb{Z}_4 \times \mathbb{Z}_6$ is not cyclic.

The maximum order of an element in $\mathbb{Z}_4$ is 4 and the maximum order for an element of $\mathbb{Z}_6$ is 6. Since $\operatorname{lcm}(4, 6) = 12$, the maximum order for any element is at most 12.

Therefore the direct product, of order 24, is not cyclic.

(b) The group $\mathbb{Z}_2 \times \mathbb{Z}_9$ is cyclic.

Previous examples suggest that $(1, 1)$ should be a generator, which we can confirm as follows.

The order of 1 in $\mathbb{Z}_2$ is 2 and the order of 1 in $\mathbb{Z}_9$ is 9. Since $\operatorname{lcm}(2, 9) = 18$, the element $(1, 1)$ has order 18 in the direct product. As the direct product has 18 elements, it is cyclic.

Solution to Exercise 2.10

By Proposition 2.10, no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ can have order greater than the least common multiple of m and n.

Since m and n are not coprime, we have that $\operatorname{lcm}(m, n) < mn$, the order of the direct product. Hence no element can generate the whole of the direct product, and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Solution to Exercise 2.11

We have $90 = 2 \times 45$. Since 2 and 45 are coprime, we can deduce from Corollary 2.12 that

$$\mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_{45}.$$

Similarly, since $45 = 9 \times 5$ and these factors are coprime, we have

$$\mathbb{Z}_{45} \cong \mathbb{Z}_9 \times \mathbb{Z}_5.$$

Combining these results gives

$$\begin{aligned} \mathbb{Z}_{90} &\cong \mathbb{Z}_2 \times \mathbb{Z}_{45} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5. \end{aligned}$$

Solution to Exercise 2.12

We use induction on r, the number of distinct prime factors, and generalise the argument used in the solution to Exercise 2.11.

Firstly, if $r = 1$ the result is immediate. Now suppose that the result is true for $r - 1$ and write

$$\begin{aligned} n &= p_1^{k_1} (p_2^{k_2} \cdots p_r^{k_r}) \\ &= n_1(n_2 \cdots n_r), \end{aligned}$$

where, because all the p_i are distinct, the factors n_1 and $n_2 \cdots n_r$ are coprime. By Corollary 2.12, we have

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2 \cdots n_r}.$$

But $\mathbb{Z}_{n_2 \cdots n_r} \cong \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ by the inductive hypothesis, hence the result holds for $\mathbb{Z}_n$ by Proposition 1.10.

Solution to Exercise 2.13

We apply Theorem 2.13 to each of the cyclic factors appearing in the direct product $\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5$. For example, since $154 = 2 \times 7 \times 11$, we have

$$\mathbb{Z}_{154} \cong \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}.$$

Hence
$$\begin{aligned} \mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5 &\cong (\mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}) \times (\mathbb{Z}_4 \times \mathbb{Z}_5) \times \mathbb{Z}_5 \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11}. \end{aligned}$$

Note that 4 is a prime power and it cannot be factorised into distinct primes.

Similarly, we apply Theorem 2.13 to each of the cyclic factors appearing in the direct product $\mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}$. This gives

$$\begin{aligned} \mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10} &\cong (\mathbb{Z}_5 \times \mathbb{Z}_{11}) \times (\mathbb{Z}_4 \times \mathbb{Z}_7) \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11}. \end{aligned}$$

Thus the two groups $\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5$ and $\mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}$ are isomorphic to the same direct product and hence to one another.

Solution to Exercise 2.14

(a) $$\begin{aligned}\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{75} &\cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_3 \times \mathbb{Z}_{25}) \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{25} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{5^2}.\end{aligned}$$

(b) $$\begin{aligned}\mathbb{Z}_9 \times \mathbb{Z}_{21} \times \mathbb{Z}_{245} &\cong \mathbb{Z}_9 \times (\mathbb{Z}_3 \times \mathbb{Z}_7) \times (\mathbb{Z}_5 \times \mathbb{Z}_{49}) \\ &\cong (\mathbb{Z}_3 \times \mathbb{Z}_9) \times \mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_{49}) \\ &= (\mathbb{Z}_3 \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_{7^2}).\end{aligned}$$

Solution to Exercise 3.1

In each case we use commutativity of addition and multiplication in P_4 to write the variables in the polynomials in a 'natural' order.

(a) $(1\,2)(3\,4) \wedge x_1x_2x_3 - x_4 = x_1x_2x_4 - x_3$

(b) $(1\,2)(3\,4) \wedge x_1x_2 - x_3x_4 = x_1x_2 - x_3x_4$

(c) $(1\,2\,3\,4) \wedge x_1 + x_2 + x_3 + x_4 = x_1 + x_2 + x_3 + x_4$

Solution to Exercise 3.2

By Definition 3.1,

$$g^{-1} \wedge y = g^{-1} \wedge (g \wedge x) = (g^{-1}g) \wedge x = e \wedge x = x.$$

Solution to Exercise 3.3

(a) Pre- and post-multiplying the equation $sr = r^{-1}s$ by r and r^{-1} respectively gives

$$\begin{aligned}sr = r^{-1}s &\Rightarrow rsr = rr^{-1}s \\ &\Rightarrow rsrr^{-1} = rr^{-1}sr^{-1} \\ &\Rightarrow rs = sr^{-1}, \quad \text{as required.}\end{aligned}$$

(b) $$\begin{aligned}rs = sr^{-1} &\Rightarrow srs = ssr^{-1} = r^{-1} \quad \text{and} \\ rs = sr^{-1} &\Rightarrow rss = sr^{-1}s \\ &\Rightarrow r = sr^{-1}s.\end{aligned}$$

(c) Recall that $s = s^{-1}$. Using the formula for the power of a conjugate preceding the exercise, and part (b), gives

$$sr^ms = (srs)^m = r^{-m}.$$

Similarly,

$$sr^{-m}s = (sr^{-1}s)^m = r^m.$$

(d) Pre-multiplying both sides of the first equation by s gives

$$sr^ms = r^{-m} \Rightarrow r^ms = sr^{-m}.$$

Post-multiplying both sides of the second equation by s gives

$$sr^{-m}s = r^m \Rightarrow r^{-m}s = sr^m.$$

Solution to Exercise 3.4

We will use the equality $s = s^{-1}$ repeatedly.

(a) $r^m \wedge r^n = r^m r^n r^{-m} = r^n$

(b)
$$\begin{aligned} r^m \wedge r^n s &= r^m (r^n s) r^{-m} \\ &= r^{m+n} s r^{-m} \\ &= r^{m+n} r^m s \text{ using } s r^{-m} = r^m s \quad \text{(from Exercise 3.3)} \\ &= r^{2m+n} s \end{aligned}$$

(c)
$$\begin{aligned} r^m s \wedge r^n &= r^m s (r^n)(r^m s)^{-1} \\ &= r^m s (r^n) s r^{-m} \\ &= r^m (s r^n s) r^{-m} \\ &= r^m r^{-n} r^{-m} \text{ using } s r^n s = r^{-n} \quad \text{(from Exercise 3.3 with } m = n\text{)} \\ &= r^{-n} \end{aligned}$$

(d)
$$\begin{aligned} r^m s \wedge r^n s &= r^m s (r^n s)(r^m s)^{-1} \\ &= r^m s (r^n s) s r^{-m} \\ &= r^m s r^n (ss) r^{-m} \\ &= r^m s r^{n-m} \quad \text{(since } ss = e\text{)} \\ &= r^m r^{m-n} s \text{ using } s r^m = r^{-m} s \quad \text{(from Exercise 3.3)} \\ &= r^{2m-n} s \end{aligned}$$

Solution to Exercise 3.5

We read the orbits from the columns of Table 3.1.

$$\begin{array}{ll} \mathrm{Orb}(e) = \{e\} & \mathrm{Orb}(s) = \{s,\ r^2 s,\ r^4 s\} \\ \mathrm{Orb}(r) = \{r,\ r^5\} & \mathrm{Orb}\left(r^2 s\right) = \{s,\ r^2 s,\ r^4 s\} \\ \mathrm{Orb}\left(r^5\right) = \{r,\ r^5\} & \mathrm{Orb}\left(r^4 s\right) = \{s,\ r^2 s,\ r^4 s\} \\ \mathrm{Orb}\left(r^2\right) = \{r^2,\ r^4\} & \mathrm{Orb}(rs) = \{rs,\ r^3 s,\ r^5 s\} \\ \mathrm{Orb}\left(r^4\right) = \{r^2,\ r^4\} & \mathrm{Orb}\left(r^3 s\right) = \{rs,\ r^3 s,\ r^5 s\} \\ \mathrm{Orb}\left(r^3\right) = \{r^3\} & \mathrm{Orb}\left(r^5 s\right) = \{rs,\ r^3 s,\ r^5 s\} \end{array}$$

Solution to Exercise 3.6

(a) $\mathrm{Orb}(x_1x_2x_3 - x_4) =$
$\{x_1x_2x_3 - x_4, x_2x_3x_4 - x_1, x_1x_3x_4 - x_2, x_1x_2x_4 - x_3\}$

(b) $\mathrm{Orb}(x_1x_2x_3x_4) = \{x_1x_2x_3x_4\}$

(c) $\mathrm{Orb}(x_1x_2 + x_3x_4) = \{x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}$

Solution to Exercise 3.7

In the column of Table 3.1 headed by s, the element s occurs 4 times. The stabiliser is

$$\mathrm{Stab}(s) = \left\{e,\ r^3,\ s,\ r^3 s\right\}.$$

Solution to Exercise 3.8

Closure Suppose that g and h are in $\mathrm{Stab}(x)$. Then

$$\begin{aligned}(gh) \wedge x &= g \wedge (h \wedge x) && \text{(by the definition of group action)}\\ &= g \wedge x && \text{(since } h \text{ fixes } x)\\ &= x && \text{(since } g \text{ fixes } x).\end{aligned}$$

Hence gh is in $\mathrm{Stab}(x)$ and $\mathrm{Stab}(x)$ is closed.

Identity By the definition of a group action, we know that $e \wedge x = x$ for any $x \in X$. This shows that e is in $\mathrm{Stab}(x)$.

Inverses Suppose $g \in \mathrm{Stab}(x)$. Then $x = g \wedge x$ and so

$$\begin{aligned}g^{-1} \wedge x &= g^{-1} \wedge (g \wedge x)\\ &= \left(g^{-1}g\right) \wedge x && \text{(by the definition of group action)}\\ &= e \wedge x\\ &= x.\end{aligned}$$

Hence $g^{-1} \in \mathrm{Stab}(x)$.

This completes the proof that $\mathrm{Stab}(x)$ is a subgroup of G.

Solution to Exercise 3.9

(a) $\mathrm{Stab}(x_1x_2^2 + x_2x_3^2 + x_1^2x_3) = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

(b) $\mathrm{Stab}(x_1x_2x_3) = S_3$

(c) $\mathrm{Stab}(x_1x_2) = \{e, (1\ 2)\}$

Solution to Exercise 3.10

(a) We can see that $g \wedge x = gx \in X = S_3$.

We check properties (a) and (b) of Definition 3.1.

(a) $e \wedge x = ex = x$ for all $x \in X$.

(b) $g \wedge (h \wedge x) = g \wedge (hx) = (gh)x = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$.

(b) $\mathrm{Orb}(e) = S_3$, so there is just one orbit.

(c) $\mathrm{Stab}((1\,2\,3)) = \{e\}$.

Solution to Exercise 3.11

(a) $\{e, s\}, \{r, rs\}, \left\{r^2, r^2s\right\}$

(b) $\mathrm{Send}_1(1) = \{e, s\}, \quad \mathrm{Send}_1(2) = \{r, rs\}, \quad \mathrm{Send}_1(4) = \left\{r^2, r^2s\right\}.$

Solution to Exercise 3.12

First we assign a number to each element of G.

$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8

Now we find the permutations given by the group action $g \wedge x = gx$.

For example, $g_3 = (2,0)$ generates the following permutation of $\mathbb{Z}_4 \times \mathbb{Z}_2$ (written using two-line notation for $\mathbb{Z}_4 \times \mathbb{Z}_2$).

$$\begin{pmatrix} (0,0) & (1,0) & (2,0) & (3,0) & (0,1) & (1,1) & (2,1) & (3,1) \\ (2,0) & (3,0) & (0,0) & (1,0) & (2,1) & (3,1) & (0,1) & (1,1) \end{pmatrix}$$

This can be written as

$$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_3 & g_4 & g_1 & g_2 & g_7 & g_8 & g_5 & g_6 \end{pmatrix},$$

or, in two-line notation for S_8 (we just remove the gs) as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix},$$

giving the permutation $(1\,3)(2\,4)(5\,7)(6\,8)$ in cycle notation.

The complete list of permutations in S_8 induced by an element of $\mathbb{Z}_4 \times \mathbb{Z}_2$ is as follows.

$(0,0) \mapsto e$
$(1,0) \mapsto (1\,2\,3\,4)(5\,6\,7\,8)$
$(2,0) \mapsto (1\,3)(2\,4)(5\,7)(6\,8)$
$(3,0) \mapsto (1\,4\,3\,2)(5\,8\,7\,6)$
$(0,1) \mapsto (1\,5)(2\,6)(3\,7)(4\,8)$
$(1,1) \mapsto (1\,6\,3\,8)(2\,7\,4\,5)$
$(2,1) \mapsto (1\,7)(2\,8)(3\,5)(4\,6)$
$(3,1) \mapsto (1\,8\,3\,6)(2\,5\,4\,7)$

This list defines a mapping that gives a homomorphism from G to a subgroup of S_8.

Solution to Exercise 3.13

(a) $g_3 = (rs)^{-1} = sr^{-1} = sr^2 = rs$. Since there are three distinct elements in the tuple, the orbit will have three elements (one for each possible permutation of the three elements).

(b) $g_3 = (r^2)^{-1} = r$. There is only one element in this orbit.

(c) The elements $(r,r,r), (e,e,e), (r^2,r^2,r^2)$ are stabilised by $(1\,2\,3)$. There can be no others, since any triple stabilised by $(1\,2\,3)$ has the form (a,a,a), so $a^3 = e$.

Solution to Exercise 3.14

(a) Since 2 and 3 are both prime and divide 6, by Cauchy's Theorem the group G has an element g of order 2 and an element h of order 3. Then the subgroups $\langle g \rangle$ and $\langle h \rangle$ are cyclic and of order 2 and 3 respectively.

(b) The product ab has order 6, and so $G = \langle ab \rangle$ is cyclic.

Solution to Exercise 3.15

Since p and d are coprime integers, there exist integers s and t such that $sp + td = 1$. Then

$$y = (sp + dt)y = s(py) + t(dy) \in A.$$

Solution to Exercise 3.16

Since $8 = 2^3$, we know from Theorem 3.19 that G is a direct product of cyclic groups. The possibilities are:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

We have not included $\mathbb{Z}_2 \times \mathbb{Z}_4$, because this group is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Chapter 7

Finite groups

Introduction

In Chapter 6 we classified cyclic groups, and abelian groups whose order is a product of distinct prime numbers. In this chapter we explore certain more general classes of finite groups, not necessarily abelian, including all groups of order up to 14.

We start by finding a method of writing group elements so that we can manipulate them in a way that generalises what we do for cyclic groups, where we can write every element as a power of a generator. In this way, we can work with larger finite groups for which writing down a Cayley table would be impractical. In the process, we introduce a new class of groups known as *dicyclic* groups.

We move on to link group actions to conjugacy and introduce the idea of the *centre* of a group G, that is, the set of all those elements that commute with every other element of G. We apply the tools at our disposal to classify groups of order p^2 and groups of order $2p$ where p is an odd prime. These results cover groups of order 4, 9, 6, 10 and 14. We then give ad hoc results for groups of order 8 and 12. In this way, and using our knowledge of the structure of groups of prime order, we obtain a classification of finite groups of order up to 14.

In the final section we explore the structure of finite groups whose order is a power of a prime p, known as *finite p-groups*.

Chapter guide

In terms of study time, Section 1 should be similar to Section 2. Section 2 builds on notions that you will begin to find familiar by now.

Section 3 is fairly theoretical: some of the proofs are quite technical, but they are particularly interesting because they make use of many results and notions from previous chapters. There are few exercises, mainly intended to provide some of the steps in the various proofs.

Section 4 is slightly shorter, with one important theorem and proof, and few exercises.

1 Describing groups

The idea that a single group element *generates* a (cyclic) subgroup by repeated applications of the group operation can be generalised to the case of a finite set of elements. This section introduces the notion of a set of generators of a group and a set of *relations* among the generators. As an example, it looks at a family of finite groups called the dicyclic groups, describing them in terms of generators and relations.

1.1 Generators and relations

A group with 12 elements, such as D_6, the symmetry group of the regular hexagon, is really too large to deal with conveniently by a Cayley table. In this section we formally introduce a way of describing a group using generators. We have been using this approach informally in the previous two chapters, and in this section we will take a more rigorous approach.

Our aim is to find a more succinct way of describing the elements of D_6 than by simply listing all 12 elements. In Chapter 6, we used this approach when working with the action of D_6 on itself by conjugation. We would like this description to aid us with manipulating elements in the same way that in $\mathbb{Z}_7$ (say) we can write any element as a power of a generator a, and can write the composition of two elements a^2 and a^3 (say) as $a^2a^3 = a^5$.

The term 'generators' is an extension of the term 'generator' that you met in the context of cyclic groups. We will start this section by describing D_6 in this way. In the following discussion, you can think of the generators as being the elements involved in our succinct description and of the relations as being the rules we need to carry out manipulations.

It is fairly easy to spot a possible generator for all the rotations: for example, the rotation anticlockwise about the centre through $\frac{\pi}{3}$ can be used to produce all the rotations (including the identity).

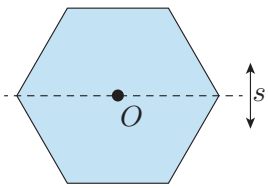


Figure 1.1 Reflection of a hexagon in a given line

Composing rotations with the same centre always produces a rotation and never a reflection. As a consequence, a set of generators of D_6 must contain a reflection, since the whole group does. Consider, for example, the reflection in the line shown in Figure 1.1.

Let us label the chosen rotation r and the chosen reflection s. In the following exercise, you are asked to show that these two elements generate D_6. In fact, as you may wish to check, the reflection s is not the only possible choice: *any* reflection will do.

In the notation of M208, $r = r_{\pi/3}$ and $s = q_0$. We have chosen shorter labels for convenience in the calculations that follow.

Exercise 1.1

Let s be the reflection of the hexagon shown in Figure 1.1, and let r be the anticlockwise rotation through $\frac{\pi}{3}$ about the centre of the hexagon.

(a) Express each of the six rotations in D_6 as powers of r.

(b) Express each of the six reflections in D_6 in the form $r^n s$, for suitable integers n.

(c) Since sr must be a group element (by the closure axiom), it must be one of the elements found in the solutions to parts (a) and (b). Which one?

The solution to Exercise 1.1 gives a description of D_6 that will make calculations with its elements much easier. The group D_6 is generated by two elements r and s about which we know the following:

$$r^6 = s^2 = e, \quad sr = r^5 s.$$

Note that the second equation can also be written

$$sr = r^{-1}s.$$

We use these equations to describe the group as follows:

$$D_6 = \langle r, s \,|\, r^6 = s^2 = e,\ sr = r^5 s \rangle.$$

In this description of D_6, the elements r and s are known as the *generators* of the group, and the equations $r^6 = s^2 = e,\ sr = r^5 s$ as the *relations*. We have further information about D_6, namely that every element can be written uniquely in the form

$$r^i s^j \quad \text{for } i = 0, \ldots, 5 \quad \text{and} \quad j = 0, 1.$$

Note that, since $r^0 = s^0 = e$, we usually write $r^i s^0$ as r^i and $r^0 s^j$ as s^j. Thus, elements of D_6 have a **standard form**. The existence of such a standard form enables computations to be made without recourse to a Cayley table.

In practice if, for a given group G, we know

- two generators a and b
- the orders of the two generators
- a relation indicating how to write ba as $a^m b^n$ for some m, n

For an abelian group, for example, we have the relation $ba = ab$.

then we have enough information to write the elements of G in a standard form $a^i b^j$.

This means that we can give an alternative complete and compact description of D_6 as follows:

$$D_6 = \{r^i s^j : i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e,\ sr = r^5 s\}.$$

Note that we have used set notation here, rather than angled brackets. This is because you can read this description of D_6 as 'the set of expressions of the form $r^i s^j$ where $i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e$ and $sr = r^5 s$'.

The information on the orders of the generators and the relation between them can be used to express any element of D_6 in standard form. As an example, here is how to find the standard form of the product $sr^2 s$.

$$\begin{aligned} sr^2 s &= srrs \\ &= r^5 srs && \text{using } sr = r^5 s \\ &= r^5 r^5 ss && \text{using } sr = r^5 s \text{ again} \\ &= r^{10} e && \text{using } s^2 = e \\ &= r^4 && \text{using } r^6 = e \end{aligned}$$

Exercise 1.2

Let $D_6 = \{r^i s^j : i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e,\ sr = r^5 s\}$.

(a) Use the relations given to express sr^2 and sr^3 in standard form.

(b) Write s^5 in standard form.

The description $D_6 = \langle r, s \mid r^6 = s^2 = e,\ sr = r^5 s\rangle$ is known as a **group presentation**. In general, a group presentation consists of a set of **generators** $g_1, g_2, \ldots, g_n$, say, and a set of equations known as **relations**. Sometimes the relations are given as expressions involving the generators that equate to the identity. Such presentations assume the existence of inverses of the generators as well as the existence of the identity e. It is possible to formally define a group presentation and to define the group described by any such presentation, but we will not do this here. We will just note the properties we need as follows.

Properties of a group presentation

Let G be a group with presentation

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m\rangle.$$

1. Any element of the group can be written in the form

   $$g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_s}^{n_s},$$

   where $i_1, \ldots, i_s \in \{1, 2, \ldots, n\}$ and $n_i \in \mathbb{Z}$. In this expression there may be repetitions of a generator, and the powers can be both positive and negative.
2. Any equation that holds in the group can be derived from the given relations.

Expressions such as $g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_s}^{n_s}$ are known as **words**.

There is a famous issue with this form of presentation, known as the *word problem*, whereby it is not always possible to know whether two words w_1 and w_2 are equal. In other words, it is not always possible to know whether the equality $w_1 = w_2$ can be derived from the given relations. Luckily, the word problem does not arise in the groups we discuss in this module.

For some groups, such as the dihedral groups, elements have a standard form.

Definition 1.1 *Standard form of elements*

Let G be a group with presentation

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m \rangle.$$

Then we say that elements of G have a **standard form** if every element of G can be written uniquely as a product of powers of the generators according to a specified pattern.

When it is possible to find a standard form for the elements of a certain group, it is also possible to give an alternative presentation of the group whereby the list of generators is replaced by the standard form of the elements of the group. We have done this above for D_6, where we have used the presentation

$$D_6 = \{r^i s^j : \ i = 0, \ldots, 5, \ j = 0, 1; \ r^6 = s^2 = e, \ sr = r^5 s\},$$

where, as remarked earlier, we use set notation rather than angled brackets.

Exercise 1.3

By what names do you know the groups with the following presentations?

(a) $\{r^i : i = 0, \ldots, 5; \ r^6 = e\}$

(b) $\{r^i s^j : i = 0, \ldots, 3, \ j = 0, 1; \ r^4 = s^2 = e, \ sr = r^3 s\}$

(c) $\{r^i s^j : i = 0, 1, \ j = 0, 1; \ r^2 = s^2 = e, \ sr = rs\}$

Recall from Section 1 of Chapter 5 that there is a whole family of dihedral groups, one for each regular polygon. The **dihedral group** D_n is the symmetry group of the regular n-gon, and it has order $2n$. As you can probably see, all dihedral groups can be described in the following way:

$$D_n = \{r^i s^j : i = 0, \ldots, n-1, \ j = 0, 1; \ r^n = s^2 = e, \ sr = r^{n-1} s\}.$$

The next exercise and example are designed to give you practice in working with this type of group presentation. You are asked to work with the dihedral group D_4. Before you start, it is worth convincing yourself that the elements of D_4 may be generated by a rotation r through $\frac{\pi}{2}$ about the centre of the square and a reflection s in an axis through the centre of the square and parallel to two of its sides.

Exercise 1.4

Let G be the group of symmetries of the square, denoted by D_4. In other words,

$$G = \{r^i s^j : i = 0, 1, 2, 3,\ j = 0, 1;\ r^4 = s^2 = e,\ sr = r^3 s\}$$
$$= \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}.$$

Let N be the set $\{e, r^2\}$.

(a) Prove that N is a normal subgroup of G.

(b) Find the set of left cosets of N in G in the form aN where $a \in G$.

(c) Using your notation in part (b), write out the Cayley table of the quotient group G/N.

Example 1.2 *D_6 and the Correspondence Theorem*

Let $D_6 = \langle r, s \mid r^6 = s^2 = e, sr = r^5 s = r^{-1} s \rangle$ and let $N = \{e, r^3\}$.

It is not difficult to check that r^3 commutes with every other element of D_6 and that $(r^3)^2 = e$, so N is a normal subgroup of D_6. This implies that the quotient D_6/N is a group, whose elements are

$$\begin{array}{lll} N & = \{e, r^3\} & = r^3 N, \\ rN & = \{r, r^4\} & = r^4 N, \\ r^2 N & = \{r^2, r^5\} & = r^5 N, \\ sN & = \{s, r^3 s\} & = r^3 sN, \\ rsN & = \{rs, r^4 s\} & = r^4 sN, \\ r^2 sN & = \{r^2 s, r^5 s\} & = r^5 sN. \end{array}$$

So $D_6/N = \{N, rN, r^2 N, sN, rsN, r^2 sN\} \cong D_3$. We now apply the Correspondence Theorem to D_6/N to understand the structure of D_6.

You can check that in this copy of D_3, the identity is N, the two non-trivial rotations are rN and $r^2 N$, and sN, rsN, $r^2 sN$ are the three reflections.

Now consider the subgroup $H = \{e, r, r^2, r^3, r^4, r^5\}$ of D_6. This subgroup contains N, and it is a normal subgroup of index 2 in D_6.

Thus, by the Correspondence Theorem, H/N is a normal subgroup of D_6/N of index 2 in D_6/N. Since $H/N = \{hN :\ h \in H\}$, the elements of H/N are as follows.

$$\begin{array}{ll} N & = \{e, r^3\} \\ rN & = \{r, r^4\} \\ r^2 N & = \{r^2, r^5\} \end{array}$$

So $H/N = \{N, rN, r^2 N\}$, which is indeed a normal subgroup of D_6/N of index 2: it corresponds to the subgroup of three rotations in D_3 (remember that the identity is a rotation through 0).

Now, the group D_3 has three non-normal subgroups of order 2 and index 3, each of which contains the identity and a reflection.

As a subgroup of D_6/N, one of these three non-normal subgroups is

$$\overline{K} = \{N, sN\}.$$

Since $(sN)^2 = s^2N = eN = N$, we know that sN is self-inverse.

By the Correspondence Theorem, D_6 has a non-normal subgroup K of index 3 that contains N and for which $K/N = \{N, sN\} = \overline{K}$. Thus K is the union of two cosets of N, namely

$$K = N \cup sN = \{e, r^3\} \cup \{s, r^3 s\} = \{e, r^3, s, r^3 s\}.$$

Confirm this by finding K/N for $K = \{e, r^3, s, r^3 s\} \subseteq D_6$.

Finally, note the following.

- K is a subgroup containing N – in fact K is isomorphic to the Klein group, or D_2.
- $|K| = 4$ so the index of K in D_6 is $|D_6|/4 = 12/4 = 3$.
- $rK = \{r, r^4, rs, r^4 s\}$ whereas $Kr = \{r, r^4, r^5 s, r^2 s\} \neq rK$, so K is not normal in D_6.

Exercise 1.5

In the notation of Example 1.2, let $\overline{K}_1$ and $\overline{K}_2$ be the two non-normal subgroups of D_6/N not equal to K.

(a) Write down the elements of $\overline{K}_1$ and $\overline{K}_2$.

(b) Find the subgroups of D_6 that contain N which correspond to $\overline{K}_1$ and $\overline{K}_2$ as in the Correspondence Theorem.

Our findings about the Correspondence Theorem for D_6 in Example 1.2 and Exercise 1.5 are illustrated in Figure 1.2.

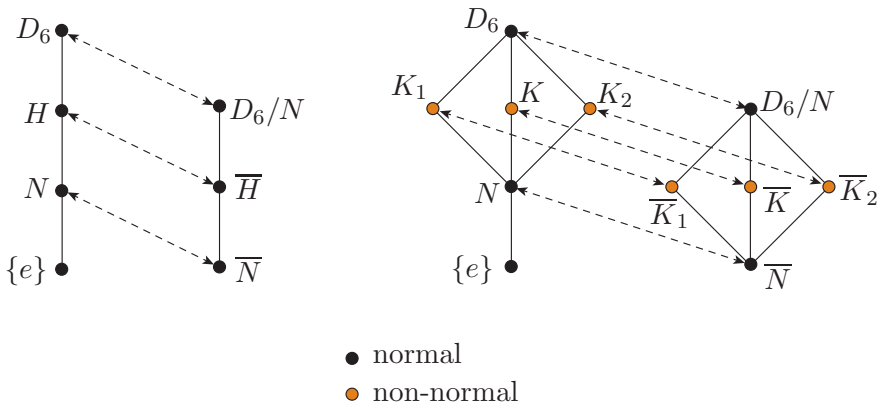


Figure 1.2 D_6 and the Correspondence Theorem

1.2 Dicyclic groups

Consider the group Dic_2 with presentation

$$\mathrm{Dic}_2 = \langle a, b \mid a^4 = e, a^2 = b^2, aba^3b = e \rangle.$$

This is the first in an important family of finite groups whose properties we will explore in this subsection.

Our first task will be to derive some properties of Dic_2 that follow from the relations $a^4 = e$, $a^2 = b^2$ and $aba^3b = e$.

Exercise 1.6

Show that the following hold in the group Dic_2:

(a) $b^4 = e$

(b) b^2 commutes with both a and b

(c) $ba = a^3b$

(d) any element g of Dic_2 can be written in the form $g = a^r b^s : \ r = 0, \ldots, 3, \ s = 0, 1$.

You may suspect, rightly, that in Exercise 1.6(d) we have found a standard form for the elements of Dic_2. However, to be sure that we really have a standard form we need to show that each element of Dic_2 can be written as $a^r b^s$, for suitable r and s, in a *unique* way.

Note that the expression $a^r b^s$ gives eight elements as r ranges over $0, \ldots, 3$ and s over $0, 1$. Thus, if we can find a group of eight elements with the given presentation, we will know that the expression $a^r b^s$ gives a standard form for its elements. You should be aware that there is no general way of finding such a group.

Consider the diagram in Figure 1.3. You may find it helpful to think of it as a dance formation or as the spokes of two wheels. In Figure 1.4 below, regard a as the dance move where the dancers (or the spokes of the two wheels) rotate anticlockwise through $\frac{\pi}{2}$.

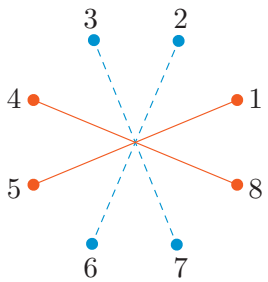


Figure 1.3 A dance formation

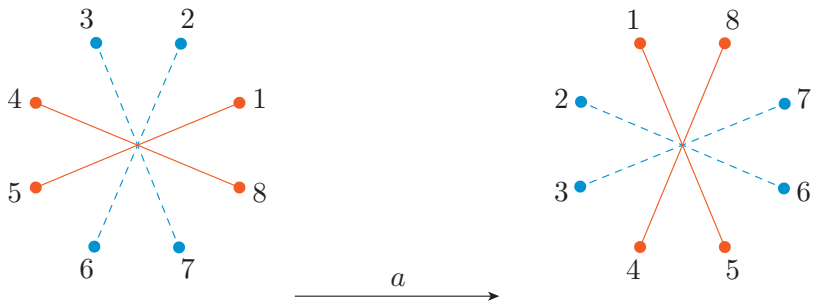


Figure 1.4 The effect of a on the dancers

Now regard b as the dance move where the two sets of dancers separate, rotate by one dancer in opposite directions and then come together again, or the move that rotates the two sets of spokes (one dashed and one solid) by one spoke but in opposite directions (Figure 1.5). The dancers (spokes) joined by solid lines move clockwise and the ones joined by a dotted line move anticlockwise.

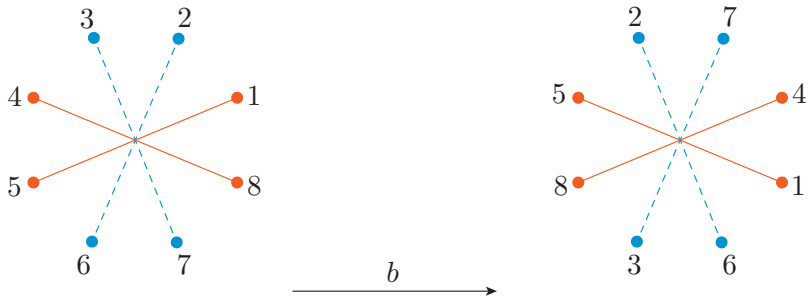


Figure 1.5 The effect of b on the dancers

If we regard a and b as permutations of the set of dancers (or spokes), these descriptions of a and b show that $a^4 = b^4 = e$. They also show that a followed by b is a permutation that reverses the direction of the dancers/spokes in b; that is, the solid lines now move anticlockwise and the dotted lines clockwise. This shows that $ba = ab^{-1} = ab^3$. Finally, you can observe that $a^2 = b^2$ (Figure 1.6).

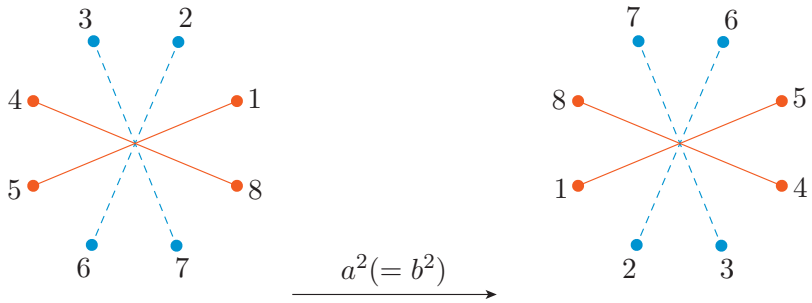


Figure 1.6 The effect of $a^2(= b^2)$ on the dancers

We have thus shown that a and b satisfy the relations in the presentation of the group Dic_2. Since the possible combinations of a and b give rise to eight different permutations of the dancers/spokes, we can see that these permutations form a group of order 8. This group is known as the **dicyclic** group of order 8. It is also known as the **quaternion group**.

In the next exercise you will see another characterisation of the group Dic_2 as a group of matrices over the complex numbers.

Recall that a **complex number** is an expression of the form

$$x + iy,$$

where x and y are real numbers and $i^2 = -1$. The set of all complex numbers is denoted by $\mathbb{C}$.

Exercise 1.7

(a) Let $\mathrm{GL}(2, \mathbb{C})$ be the group of invertible 2×2 matrices over the complex numbers, and let G be the subgroup of $\mathrm{GL}(2, \mathbb{C})$ whose generators are

$$a = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Show that $G \cong \mathrm{Dic}_2$.

(b) Show that G has three normal cyclic subgroups of order 4.

The quaternions are an extension of the complex numbers, and they were first described by the Irish mathematician Sir William Rowan Hamilton (1805–1865). A key fact about this extension is that it is a group where multiplication is not commutative. The quaternion group is the smallest multiplicative subgroup containing the three elements often known as i, j, k, where

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = k, jk = i, ki = j.$$

The reason why Dic_2 has two names is that it is the smallest in a family of groups known as the *dicyclic groups*. The dance or wheel pictures help us to describe this family. Consider a dance formation with $4n$ dancers, or a pair of wheels with $4n$ spokes, $2n$ of which are dotted and $2n$ solid. The dancers, or spokes, are divided into four blocks with n dancers or spokes in each, arranged so that the dotted blocks are opposite one another and the solid blocks are opposite one another.

As before, we regard a as the dance move where the dancers, or spokes, rotate anticlockwise by $\frac{\pi}{2}$ (Figure 1.7).

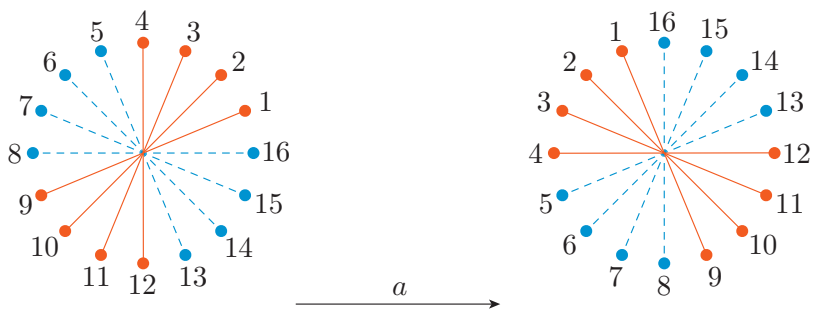


Figure 1.7 The effect of a on a formation of 16 dancers

Again, regard b as the dance move where the two sets of dancers separate, rotate by one dancer in opposite directions and then come together again, or the move that rotates the two sets of spokes (one dashed and one solid) by one spoke but in opposite directions (Figure 1.8). The dancers/spokes joined by solid lines move clockwise, and the ones joined by dotted lines move anticlockwise.

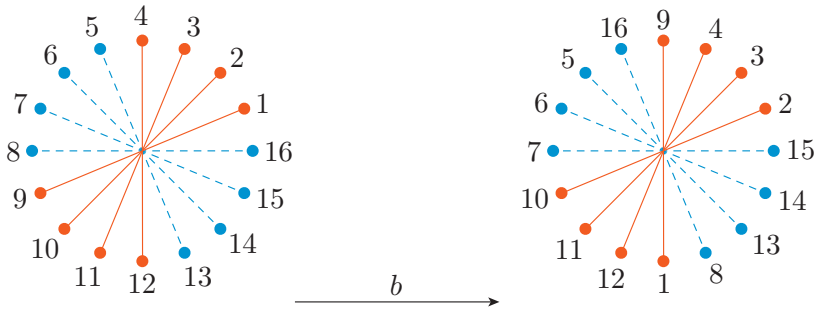


Figure 1.8 The effect of b on a formation of 16 dancers

We can see that in the general case of $4n$ dancers/spokes,

$$a^4 = e, \quad b^{2n} = e \quad \text{and} \quad a^2 = b^n.$$

Some thought may enable you to see that $ab = b^{-1}a$ or, equivalently, $aba^3b = e$. We can therefore give a presentation of the group described using $4n$ dancers/spokes as the **dicyclic group**

$$\mathrm{Dic}_n = \langle a, b \mid a^4 = e, a^2 = b^n, aba^3b = e \rangle.$$

Note that there are $4n$ possible positions of the dancers/spokes, so this group has order $4n$.

Adding dicyclic groups to our list of 'known' groups will enable us, by the end of this chapter, to describe all groups of order up to 14.

Exercise 1.8

Show that elements of Dic_n have a standard form given by

$$a^r b^s \quad \text{for } r = 0, \ldots, 3, \ s = 0, \ldots, n-1.$$

1.3 Describing subgroups using generators

We have used many times the idea of a subgroup *generated* by a particular element x of a group. Such a subgroup is a cyclic group denoted by $\langle x \rangle$, and its elements can be described precisely as follows:

$$\langle x \rangle = \{x^n : \ n \in \mathbb{Z}\}.$$

It is also possible to consider generating sets with more than one element, and in fact this is what we have done implicitly in Subsections 1.1 and 1.2

when working with generators in group presentations. For such generating sets, the situation becomes slightly more complex and much more interesting. Informally, we say that the subgroup of a group G generated by a set S is the smallest subgroup of G that contains S. By 'smallest', we mean a subgroup of G containing S that is contained in every other subgroup that contains S.

In what follows, we deal with the problem of whether such subgroups exist and what their elements look like.

Definition 1.3 *Subgroup generated by a set*

Let G be a group and S be a subset of (the underlying set of) G. We define the **subgroup H of G generated by S** to be a subgroup of G satisfying:

(a) $S \subseteq H$

(b) if K is a subgroup of G and $S \subseteq K$ then $H \subseteq K$.

We denote this subgroup by $\langle S \rangle$.

The notation $\langle S \rangle$ is a generalisation of the notation $\langle x \rangle$ used for cyclic subgroups generated by the single element x. To be consistent, we ought to change the previous notation to $\langle \{x\} \rangle$, though, like most mathematicians, we will not do so.

In the next lemma we prove the existence of subgroups generated by a set.

Lemma 1.4

Let G be a group and S be a subset of (the underlying set of) G. Then the group generated by S exists and is unique.

Proof To prove existence, consider the collection of all subgroups of G that contain the set S. This collection is certainly non-empty, since it contains the subgroup G.

Now, by Proposition 2.7 of Chapter 5, the intersection H of all of these subgroups is itself a subgroup of G. Furthermore, since each of the subgroups in the collection contains the set S, so does their intersection H. So H is a subgroup of G containing S.

In addition, if any subgroup of G contains the set S, it is in our collection and so it must contain the intersection H.

So H is a subgroup of G generated by S.

For uniqueness, suppose there is another subgroup J generated by S. Then $H \subseteq J$ and $J \subseteq H$ by condition (b) in Definition 1.3. Hence the two subgroups H and J are equal. This shows that the subgroup generated by S is unique. ■

Although Definition 1.3 and Lemma 1.4 cover infinite groups and infinite generating sets, in this module we will only be using them where the group is finite.

Worked Exercise 1.5

Consider the dicyclic group $\mathrm{Dic}_3 = \langle a, b \mid a^4 = e, a^2 = b^3, aba^3b = e\rangle$ and let $S = \{a^2, b^2\}$.

Find $H = \langle S\rangle$, the subgroup of Dic_3 generated by S.

Solution

Since Dic_3 has order 12, Lagrange's Theorem tells us that the group H must have order 2, 3, 4, 6 or 12.

Secondly, since a^2 has order 2, b^2 has order 3 and $a^2b^2 = b^2a^2$, we have that a^2b^2 has order 6 and so it generates a cyclic subgroup of order 6. We claim that $H = \langle a^2b^2\rangle$.

Now $\langle a^2b^2\rangle$ contains both $a^2 = (a^2b^2)^3$ and $b^2 = (a^2b^2)^4$. Thus H is contained in $\langle a^2b^2\rangle$.

But $\langle a^2b^2\rangle$ is contained in H, so $H = \langle a^2b^2\rangle$.

Since $a^2b^2 = b^5$, we have that H is in fact the cyclic group

$$\{e, b, b^2, b^3, b^4, b^5\}.$$

In standard form the elements of H are

$$\{e, b, b^2, a^2, a^2b, a^2b^2\}.$$

There is no systematic process to find the subgroup generated by a given subset of a group. The approach used in the previous exercise – that is, to find a subgroup containing the set and then show that this is the required subgroup – is typical of the arguments we can use.

Recall that the *alternating group* A_4 is the subgroup of S_4 consisting of the even permutations.

Exercise 1.9

Let $S = \{(1\,2\,3), (1\,2)(3\,4)\}$. Show that $\langle S\rangle = A_4$.

Before formally defining the subgroup generated by a subset S of a group G, we worked with the subgroup containing all products of powers of elements in S. The next proposition shows that this subgroup is in fact $\langle S\rangle$.

Lemma 1.6

Let G be a group and let S be a non-empty finite subset of G. Then the set

$$H = \{s_1^{r_1} \cdots s_n^{r_n} : n \in \mathbb{N},\ s_i \in S,\ r_i \in \mathbb{Z}, i = 1, \ldots, n\}$$

is a subgroup of G.

Proof We use the subgroup criterion, Proposition 2.4 of Chapter 5.

First, let $s \in S$. Then $e = s^0 \in H$ and so H is non-empty.

Now let $x, y \in H$. Then $x = s_1^{r_1} \cdots s_m^{r_m}$ and $y = t_1^{r_1} \cdots t_n^{r_n}$ where $s_i, t_j \in S$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Then

$$xy^{-1} = s_1^{r_1} \cdots s_m^{r_m} t_n^{-r_n} \cdots t_1^{-r_1} \in H.$$

Hence H is a subgroup as required. ■

Proposition 1.7

Let G be a group, let S be a non-empty finite subset of G and let

$$H = \{s_1^{r_1} \cdots s_n^{r_n} : n \in \mathbb{N}, s_i \in S, r_i \in \mathbb{Z}, i = 1, \ldots, n\}.$$

Then the subgroup generated by S is the whole of H, that is,

$$\langle S \rangle = H.$$

Proof By Lemma 1.6, the set H is a subgroup of G. Clearly the set contains S. Moreover, by closure, any subgroup containing S must contain all possible products of powers of S and so contain H. Hence $\langle S \rangle = H$ from Definition 1.3. ■

Exercise 1.10

Let $G = S_5$ and let $a = (1\,2\,3\,4\,5), b = (2\,5)(3\,4)$. Show that $bab^{-1} = a^4$ and hence that

$$H = \langle a, b \rangle = \{a^r b^s : r = 0, \ldots, 4, s = 0, 1\}.$$

Deduce that H is a subgroup of G of order 10.

2 Conjugates, centralisers and centres

Chapter 5 reminded you about conjugacy and normal subgroups. In Chapter 6 you saw that conjugation allows us to define a group action of D_6 on itself. This section looks at conjugation and related ideas in a little more detail.

As you may recall from your previous studies, conjugation brings out similarities between group elements. For example, in the symmetric group S_4 there are eight 3-cycles that can be regarded as being similar in some sense. In the dihedral group D_5 it is reasonable to regard all the reflections as being similar, but is the same true for the reflections in D_6? It is certainly the case that rotations in D_6 are not necessarily similar since they can have different orders. However, rotations of the same order are similar. One aim of this section is to formalise this notion of similarity. The ideas involved in this have some striking consequences for group theory in general.

2.1 Conjugates

Recall from Chapter 5, Definition 3.9, that two elements a and b of a group G are *conjugate* in G if there is $g \in G$ such that $b = gag^{-1}$. In this case, we also say that gag^{-1} is the **conjugate of a by g**. Conjugacy by a given element of G can be used to define an isomorphism of G to itself.

Proposition 2.1

Let G be a group and let $g \in G$. Then the function $\phi : G \to G$, which sends each element a to its conjugate by g, that is,

$$\phi : a \mapsto gag^{-1},$$

is an isomorphism.

Proof Let $a, b \in G$. Then

$$\phi(a)\phi(b) = gag^{-1}gbg^{-1} = gabg^{-1} = \phi(ab).$$

Thus ϕ is a homomorphism.

Now consider the function $\psi : G \to G$ defined by

$$\psi : a \mapsto g^{-1}ag;$$

that is, the function that maps a to its conjugate by g^{-1}. We have

$$\psi \circ \phi\,(a) = \psi(gag^{-1}) = g^{-1}(gag^{-1})g = a.$$

Similarly, $\phi \circ \psi\,(a) = a$, so ψ is the inverse for ϕ, hence ϕ is an isomorphism, as required. ■

In the following exercise, recall that the dihedral group D_n has presentation

$$D_n = \langle r, s \mid r^n = s^2 = e, sr = r^{n-1}s \rangle,$$

and each of its elements can be expressed in the standard form $r^i s^j$ for $i = 0, \ldots, n-1$ and $j = 0, 1$.

Exercise 2.1

Compute the following conjugates, giving your answers in standard form.

(a) srs^{-1} and rsr^{-1} in D_5

(b) srs^{-1} and rsr^{-1} in D_6

2.2 Conjugacy classes

In Chapter 6, Section 3, we saw how the orbits of a group action partition the set being acted on and so they define an equivalence relation. In Proposition 3.6 in the same chapter, we also saw that conjugation can be used to define an action of D_6 on itself. This action can be generalised to give an action of any group on itself. This is the action that we will look at in detail in this subsection.

Theorem 2.2

Let G be a group. Then G acts on G by the rule

$$g \wedge a = gag^{-1} \quad \text{for all } a, g \in G,$$

and we say that G **acts on itself by conjugation**.

Proof We check that the conditions in Definition 3.1 of Chapter 6 are satisfied. First of all, it is clear that $g \wedge a \in G$ for all $a, g \in G$. Moreover:

(a) $e \wedge a = eae^{-1} = a$ for every $a \in G$

(b) $(gh) \wedge a = ghah(gh)^{-1} = ghah^{-1}g^{-1} = g \wedge (hah^{-1}) = g \wedge (h \wedge a)$ for all $g \in G, h \in G$ and all $a \in G$. ■

The action defined in Theorem 2.2 partitions G into orbits whose elements are conjugate to each other, and thus similar in some sense. The orbits turn out to be certain familiar subsets of G that you met in Chapter 5: they are the conjugacy classes of G. Thus, in the context of actions by conjugation, conjugacy classes can be defined as follows.

Definition 2.3 *Conjugacy class*

Let G be a group and $a \in G$. Then the orbit of a in the action of G on itself by conjugation is written $\mathrm{Conj}_G(a)$ and it is called the **conjugacy class** of a in G. Thus

$$\mathrm{Conj}_G(a) = \{gag^{-1} : g \in G\}.$$

Example 2.4 *Conjugacy in S_3*

The symmetric group S_3 has three transpositions, $(1\,2), (1\,3)$ and $(2\,3)$, and two 3-cycles, $(1\,2\,3)$ and $(1\,3\,2)$.

If you calculate the conjugate $\sigma(1\,2)\sigma^{-1}$ for each $\sigma \in S_3$, you should obtain the three transpositions, each occurring twice.

The conjugates of $(1\,2\,3)$ are the two 3-cycles, and the only conjugate of the identity permutation is e itself. Thus, the conjugacy classes in S_3 are

$$\{(1\,2), (1\,3), (2\,3)\},\ \{(1\,2\,3), (1\,3\,2)\} \text{ and } \{e\}.$$

In Example 2.4, the conjugacy classes partition the group S_3. This is an instance of one of several general properties of conjugacy classes, the most important of which are given below. Most of these properties can be deduced from those of general equivalence classes.

Proposition 2.5

Let G be a group. Then:

(a) for each element a of G, $a \in \mathrm{Conj}_G(a)$

(b) for $a, b \in G$, $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$ if, and only if, b is a conjugate of a

(c) $\mathrm{Conj}_G(e) = \{e\}$ for any group G

(d) all the elements of a conjugacy class have the same order

(e) if G is finite of order n, then the number of elements in a conjugacy class must divide n.

Proof

(a) This holds because $a = eae^{-1}$.

(b) Suppose that b is a conjugate of a. Then $b = xax^{-1}$ for some $x \in G$, so $x^{-1}bx = a$. Now if $c \in \mathrm{Conj}_G(a)$, then $c = dad^{-1}$ for some $d \in G$ and so

$$c = dx^{-1}bxd^{-1} = (dx^{-1})b(dx^{-1})^{-1} \in \mathrm{Conj}_G(b).$$

Thus $\mathrm{Conj}_G(a) \subseteq \mathrm{Conj}_G(b)$. The reverse inclusion is proved similarly. This shows that if b is a conjugate of a, then $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$.

Now suppose that $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$. Then since $b \in \mathrm{Conj}_G(b)$ by statement (a), $b \in \mathrm{Conj}_G(a)$ and so b is a conjugate of a.

We have proved that $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$ if, and only if, b is a conjugate of a.

(c) This follows from the fact that $geg^{-1} = e$ for all $g \in G$.

(d) From Proposition 2.1 and Theorem 4.6 of Chapter 5, we see that a and gag^{-1} have the same order. The result follows.

(e) This follows from the Orbit–Stabiliser Theorem (Corollary 3.13 of Chapter 6), since a conjugacy class is an orbit under a group action. ■

Since any group G is partitioned into its conjugacy classes, when G is finite the total number of elements in G must be the sum of the numbers of elements in each conjugacy class. This gives the following theorem.

Theorem 2.6

Let G be a finite group and let $C_1, C_2, \ldots, C_k$ be its distinct conjugacy classes. Then

$$|G| = |C_1| + |C_2| + \cdots + |C_k|.$$

Proof This follows from the fact that the conjugacy classes of G partition the group (Proposition 3.11(b) of Chapter 5). ■

The equation in Theorem 2.6 is usually called the **class equation** for G. From Exercise 3.6 of Chapter 5 we see that the class equation for S_3 is

$$6 = 1 + 3 + 2.$$

When working out the conjugacy classes of a given group, you can speed up calculations by noting the following.

- Since the identity e commutes with every other element, its conjugacy class is the set $\{e\}$. More generally, if g is any group element that commutes with every other element, its conjugacy class is $\{g\}$.
- Since conjugacy classes are orbits, their size must divide the order of the group.

Exercise 2.2

For each of the following groups, find the conjugacy classes and hence write down the class equation.

(a) $D_4 = \{r^i s^j : i = 0, \ldots, 3,\ j = 0, 1;\ r^4 = s^2 = e,\ sr = r^3 s\}$

(b) $\mathrm{Dic}_2 = \{a^i b^j : i = 0, \ldots, 3,\ j = 0, 1;\ a^4 = e, a^2 = b^2, aba^3b = e\}$

Exercise 2.2(a) shows that in the dihedral group D_4, conjugacy distinguishes between the two reflections rs and $r^3 s$, which form one class, and the other two reflections, s and $r^2 s$. Depending on the choice of s, one pair will be reflections in the diagonals and the other pair reflections in the lines joining midpoints of opposite sides. The elements s and rs, both of order 2, are *not* conjugate in D_4.

2.3 Centralisers

We have seen that conjugation gives a group action whose orbits are the conjugacy classes. In this subsection we will look at the *stabilisers* of this action. Recall that the stabiliser of an element a of a group G consists of those elements g of G such that $gag^{-1} = a$.

Definition 2.7 *Centraliser*

Let G be a group and $a \in G$. Then the stabiliser of a in the action of G on itself by conjugation is called the **centraliser** of a in G and it is written $\mathrm{Cent}_G(a)$. Thus

$$\mathrm{Cent}_G(a) = \{g \in G : gag^{-1} = a\}.$$

If the group is clear from the context, the subscript G can be omitted from the notation $\mathrm{Cent}_G(a)$.

If $gag^{-1} = a$ then multiplying by g on the right gives $ga = ag$. Conversely, if $ga = ag$, then multiplying by g^{-1} on the right gives $gag^{-1} = a$. Therefore

$$gag^{-1} = a \quad \text{if, and only if,} \quad ga = ag.$$

Thus

$$\mathrm{Cent}_G(a) = \{g \in G : ga = ag\},$$

so in fact the centraliser of a in G consists of all the elements of G that commute with a.

Since $\mathrm{Cent}_G(a)$ is a stabiliser in a group action, it is always a subgroup of G (see Exercise 3.8 of Chapter 6). For example, in D_4 the centraliser of r must contain e, r, r^2, r^3, as all these elements commute with r. Since s does not commute with r, the centraliser of r cannot be the whole group. By Lagrange's Theorem, it must have order 1, 2, 4 or 8, so

$$\mathrm{Cent}_{D_4}(r) = \{e, r, r^2, r^3\}.$$

It is always true that $\langle a \rangle \subseteq \mathrm{Cent}_G(a)$, because $aa^i = a^{i+1} = a^i a$ for all integers i, but in the next exercise you will see examples where $\langle a \rangle \neq \mathrm{Cent}_G(a)$.

Exercise 2.3

Find the following centralisers. In each case, state whether $\mathrm{Cent}_G(a) = \langle a \rangle$.

(a) $\mathrm{Cent}_{S_3}(1\,2\,3)$ and $\mathrm{Cent}_{S_3}(1\,2)$

(b) $\mathrm{Cent}_{D_4}(r^2)$ and $\mathrm{Cent}_{D_4}(s)$

Exercise 2.4

(a) If G is an abelian group, what can you say about the centraliser of any element of G?

(b) What is the centraliser of the identity element e_G in any group G?

2.4 Centres

In Exercises 2.3 and 2.4, we saw examples where a centraliser $\mathrm{Cent}_G(a)$ is the whole group G. In other words, the element a commutes with every element of G. Such elements are important enough to deserve some specific terminology.

Definition 2.8 *Central elements*

Let G be a group, and let $a \in G$ be an element that commutes with every other element of G. Then a is said to be a **central element** in G.

The set of all central elements in G is called the **centre** of G and it is denoted by $Z(G)$. Thus

$$Z(G) = \{a \in G : ga = ag \text{ for all } g \in G\}.$$

An element a of G is central in G if, and only if, $a \in \mathrm{Cent}_G(g)$ for all $g \in G$. In other words, the centre of the group is the intersection of all the centralisers. From this description, it is possible to deduce that $Z(G)$ is a subgroup of G, but we will check this directly from the subgroup criterion, Proposition 2.4 of Chapter 5. Indeed, we will go a step further and show that $Z(G)$ is in fact a normal subgroup.

Proposition 2.9

Let G be a group. Then the centre $Z(G)$ is a normal subgroup of G.

Proof We first observe that if $xg = gx$, then multiplying both sides of the equation on the left and on the right gives

$$x^{-1}xgx^{-1} = x^{-1}gxx^{-1};$$

that is, $gx^{-1} = x^{-1}g$. Now:

- For all g in G, we have $ge = eg$, so $e \in Z(G)$ and $Z(G) \neq \emptyset$.
- Let $x, y \in Z(G)$. Thus, for all $g \in G$ we have $gx = xg$ and $gy = yg$. Then

  $$g(x^{-1}y) = (gx^{-1})y = (x^{-1}g)y = x^{-1}(gy) = x^{-1}(yg) = (x^{-1}y)g,$$

  thus $g(x^{-1}y) = (x^{-1}y)g$ for all $g \in G$. That is, $x^{-1}y \in Z(G)$.

Therefore $Z(G)$ is a subgroup of G by the subgroup criterion.

Now let $a \in Z(G)$ and $g \in G$. Then $gag^{-1} = a \in Z(G)$ so that $Z(G)$ is a normal subgroup of G by Proposition 3.7 of Chapter 5. ■

Exercise 2.5

Let G be a group with centre $Z(G)$ and let H be a subgroup of $Z(G)$. Show that H is a normal subgroup of G.

There are several different ways of saying that an element is central in a group. For convenience we list them in a proposition.

Proposition 2.10

Let G be a group and let $a \in G$. The following are equivalent ways of saying that a is central in G.

(a) $ga = ag$ for all $g \in G$

(b) $\mathrm{Cent}_G(a) = G$

(c) $a \in \mathrm{Cent}_G(g)$ for all $g \in G$

(d) $gag^{-1} = a$ for all $g \in G$

(e) $\mathrm{Conj}_G(a) = \{a\}$

The significance of some of these conditions will hopefully become clear as you meet more examples and results about conjugacy classes and centralisers: loosely speaking, having many conjugates in G is the opposite of commuting with many elements of G. This remark is justified by the equivalence between conditions (a) and (d) in Proposition 2.10: an element a is equal to its conjugate by g if, and only if, a and g commute.

The centre of an abelian group is the whole group. On the other hand, the centre of a group may be the trivial subgroup, as you can see in the next exercise. The order of the centre of a group, relative to the order of the whole group, is a measure of how close the group is to being abelian.

Exercise 2.6

(a) Write down the elements of S_3 that commute with $(1\,3)$, that is, write down $\mathrm{Cent}_{S_3}(1\,3)$.

(b) Hence find $Z(S_3)$.

2.5 Conjugates and centralisers

In Chapter 6, the Orbit–Stabiliser Theorem gave a connection between orbits and stabilisers. In the context of the action of a group G on itself by conjugation, the Orbit–Stabiliser Theorem gives a connection between conjugacy classes (the orbits) and centralisers (the stabilisers). In particular, when G is finite, the finite form of the theorem, namely

$$|\mathrm{Orb}_G(a)| \times |\mathrm{Stab}_G(a)| = |G|,$$

gives the formula below.

Theorem 2.11

For any element a of any finite group G,

$$|\mathrm{Conj}_G(a)| \times |\mathrm{Cent}_G(a)| = |G|.$$

Proof The result follows from the Orbit–Stabiliser Theorem (Corollary 3.13 of Chapter 6) and Theorem 2.2. ■

In particular, Theorem 2.11 tells us that $|\mathrm{Conj}_G(a)|$ is always a factor of $|G|$, and that it is inversely proportional to $|\mathrm{Cent}_G(a)|$. In a group where we have already calculated conjugacy classes, such as S_n, this result enables us to quickly calculate centralisers and centres.

Example 2.12 *Centralisers and centre in S_n*

You may remember from your previous studies that in S_n any two cycles of the same length are conjugate.

The number of different n-cycles in S_n is $(n-1)!$ and so the conjugacy class of the cycle $\sigma = (1\,2\,\ldots\,n)$ contains $(n-1)!$ elements.

σ is the Greek letter 'sigma'.

Hence the centraliser $\mathrm{Cent}(\sigma)$ has order

$$n = \frac{n!}{(n-1)!} = n,$$

and so $\mathrm{Cent}(\sigma)$ must be the cyclic subgroup $\langle(1\,2\,\ldots\,n)\rangle$.

Now let $\tau = (1\,2\,\ldots\,(n-1))$. The conjugates of τ in S_n are the cycles ρ of length $n-1$. How many of these are there? There are n choices for the number that does not appear in ρ and, for each of these, there are $(n-2)!$ different $(n-1)$-cycles. Thus τ has $n \times (n-2)!$ conjugates and so its centraliser has order $n-1$.

τ is the Greek letter 'tau'.

ρ is the Greek letter 'rho'.

Any element in the centre of S_n must commute with both σ and τ, and so must be in $\mathrm{Cent}(\sigma) \cap \mathrm{Cent}(\tau)$. As the highest common factor of n and $n-1$ is 1, it follows that

$$\mathrm{Cent}(\sigma) \cap \mathrm{Cent}(\tau) = \{e\}.$$

Consequently, the centre of S_n is the trivial subgroup $\{e\}$.

Exercise 2.7

Recall that Dic_2 has presentation

$$\mathrm{Dic}_2 = \langle a, b \mid a^4 = e, a^2 = b^2, aba^3b = e \rangle.$$

The conjugacy classes are as follows:

$$\{e\}, \{a^2\}, \{a, a^3\}, \{ab, a^3b\}, \{b, a^2b\}.$$

(a) Write down $Z(\mathrm{Dic}_2)$.

(b) Write down $\mathrm{Conj}_{\mathrm{Dic}_2}(a)$.

(c) Hence find $\mathrm{Cent}_{\mathrm{Dic}_2}(a)$.

Theorem 2.11 and the class equation have a striking theoretical consequence. We have just seen that certain familiar groups have trivial centres. However, sometimes the nature of the order of the group precludes this possibility.

Theorem 2.13

Let G be a group of prime power order, that is,

$$|G| = p^n$$

for some prime number p and positive integer n.

Then G has a non-trivial centre.

Proof Let $C_1, C_2, \ldots, C_k$ be a list of the different conjugacy classes of G, numbered so that $C_1 = \mathrm{Conj}_G(e) = \{e\}$. Thus $|C_1| = 1$. We aim to show that there is at least one other conjugacy class with a single element a, say, $a \neq e$ so that a is central by Proposition 2.10.

The class equation for G says that $p^n = 1 + |C_2| + |C_3| + \cdots + |C_k|$.

By Theorem 2.11, each $|C_i|$ is a factor of $|G| = p^n$. As p is prime, the only factors of p^n are $1, p, p^2, \ldots, p^{n-1}$ and p^n. It is impossible for $|C_2|, |C_3|, \ldots, |C_k|$ all to be multiples of p because, if they were, then 1 would be a multiple of p. Hence $|C_i| = 1$ for some $i > 1$. As noted above, if $C_i = \{a\}$ then $a \neq e$ and a is central. Thus $Z(G) \neq \{e\}$. ■

A group to which this theorem can be applied is D_4, whose order is the prime power $8 = 2^3$. The theorem tells us that, in contrast to S_4, the dihedral group D_4 must have non-trivial centre. The element r^2 is central, and the class equation for D_4 is

$$8 = 1 + 1 + 2 + 2 + 2.$$

The idea behind the proof of Theorem 2.13 is illustrated by the fact that it is impossible to express 8 as a sum of 1s, 2s, 4s and 8s with exactly one 1.

2.6 Groups of order p^2

This subsection provides an example of the role of quotient groups in group theory: we will use certain quotients to prove that whenever p is a prime number, all groups of order p^2 are abelian.

The basic idea in using quotient groups is to obtain information about a group G from a normal subgroup N and the quotient G/N. We will do this in the case where N is the centre of G. The group $Z(G)$ is abelian because any element of $Z(G)$ commutes with every element of G, and hence with every element of $Z(G)$. Moreover, we know from Proposition 2.9 that $Z(G)$ is normal, hence we can form the quotient group $G/Z(G)$.

Theorem 2.14

If G is a group such that $G/Z(G)$ is cyclic, then G is abelian.

Proof Let $Z = Z(G)$ and let gZ be a generator of G/Z. Then every element of G/Z, that is every coset of Z, has the form $(gZ)^m = g^m Z$ for some $m \in \mathbb{Z}$. But the cosets of Z give a partition of G, so each element a of G is in one of these. If $a \in g^m Z$, then $a = g^m z$ for some $m \in \mathbb{Z}$.

Now let $a, b \in G$. Then $a = g^{m_1} z_1$ and $b = g^{m_2} z_2$ for some $m_1, m_2 \in \mathbb{Z}$ and some $z_1, z_2 \in Z$. Since z_1 and z_2 commute with every element of G and powers of g commute with each other,

$$ab = g^{m_1+m_2} z_1 z_2 = ba.$$

Thus G is abelian. ■

Theorem 2.15

If p is a prime number, then every group G of order p^2 is abelian.

Proof Let Z be the centre of G. We have to show that $Z = G$.

By Lagrange's Theorem, $|Z|$ must be one of 1, p, p^2, as these are the only factors of p^2. By Theorem 2.13, the centre Z is non-trivial; that is, $|Z| \neq 1$.

Suppose that $|Z| = p$. The quotient group G/Z has order $\frac{p^2}{p} = p$. Then G/Z is cyclic by Exercise 4.8 of Chapter 5. Theorem 2.14 then says that G must be abelian, that is $|Z| = |G| = p^2$, which contradicts the assumption $|Z| = p$. Thus the possibility $|Z| = p$ does not arise.

The only remaining possibility is that $|Z| = p^2$ and so $Z = G$. Hence G is abelian. ■

3 Groups of small order

This section classifies all groups of order up to 14, as well as all those groups whose order is a prime, twice a prime or the square of a prime. In other words, for these orders, we give a list of groups such that every group of one of those orders is isomorphic to one of the groups in the list. In order to achieve the classification, we will use the following theorems:

- from Chapter 5, Lagrange's Theorem and its consequences that the order of any element of a finite group G divides $|G|$ and that every group of prime order is cyclic
- from Chapter 6, Cauchy's Theorem (Theorem 3.16) and Theorem 1.5 on recognising direct products
- from this chapter, Theorem 2.15, which tells us that every group whose order is a square of a prime is abelian.

3.1 Groups of order p

Let p be a prime number and G be a group of order p. Then G is cyclic by Exercise 4.8 of Chapter 5. Thus we have the following proposition.

Proposition 3.1

Let p be a prime number and G be a group of order p. Then

$G \cong \mathbb{Z}_p$.

This proposition applies to all groups of orders 2, 3, 5, 7, 11 and 13.

3.2 Groups of order p^2 revisited

Let p be a prime number. We know from Theorem 2.15 that all groups of order p^2 are abelian. We also know from Theorem 3.19 of Chapter 6 that all abelian groups of order p^2 are direct products of cyclic groups. Therefore we have the following result.

Theorem 3.2

Let p be a prime number. Then every group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof Let G be a group of order p^2. Then G is abelian by Theorem 2.15.

If G is cyclic, then $G \cong \mathbb{Z}_{p^2}$.

If G is not cyclic, it is a direct product of proper cyclic subgroups by Theorem 3.19 of Chapter 6. Any non-trivial proper subgroup of G must have order p and so be isomorphic to $\mathbb{Z}_p$. Hence $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. ■

Theorem 3.2 applies in particular to groups of orders 4 and 9.

3.3 Groups of order $2p$

Among the groups whose order is less than or equal to 14, we do not yet have a classification for those of order 6, 10 and 14. These orders all have the form $2p$, where p is an odd prime.

We have already met some groups of order $2p$, for example the cyclic group $\mathbb{Z}_{2p}$, the direct product $\mathbb{Z}_p \times \mathbb{Z}_2$ and the dihedral group D_p. Theorem 2.11 of Chapter 6 tells us that

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_p \times \mathbb{Z}_2,$$

so our known examples of non-isomorphic groups of order $2p$ only really include $\mathbb{Z}_{2p}$ and D_p.

The aim of this subsection is to show that any non-cyclic group of order $2p$ is isomorphic to the dihedral group D_p.

We start by looking at certain basic properties of the dihedral group D_n of order $2n$. At the beginning of this chapter we remarked that

$$D_n = \{r^i s^j : \ i = 0, \ldots, n-1, \ j = 0, 1; \ r^n = s^2 = e, \ sr = r^{n-1}s\}.$$

Lemma 3.3

Let G be a group of even order $2n$. Suppose that G has an element a of order n and an element b of order 2 with $b \notin \langle a \rangle$. Then:

(a) $bab^{-1} = a^k$ for some integer k such that $0 < k < n$ and n is a factor of $k^2 - 1$

(b) if $n \geq 3$ and $bab^{-1} = a^{n-1}$, then $G \cong D_n$.

Proof Let $H = \langle a \rangle$. Then H has order n and index 2 in G.

(a) Exercise 3.3 of Chapter 5 tells us that H is normal in G. So $bab^{-1} \in H$, and

$$bab^{-1} = a^k$$

for some integer k with $0 \leq k < n$.

Clearly $k \neq 0$, for otherwise $ba = b$ and $a = e$. Now b has order 2 so

$$b^2 = b^{-2} = e.$$

Therefore
$$\begin{aligned} a = b^2ab^{-2} &= b(bab^{-1})b^{-1} \\ &= b(a^k)b^{-1} \\ &= (bab^{-1})^k \\ &= (a^k)^k = a^{k^2}. \end{aligned}$$

Multiplying both sides of this equality on the right by a^{-1} gives $e = a^{k^2-1}$. As a has order n, it follows from Proposition 4.5 of Chapter 5 that n divides $k^2 - 1$.

(b) As H has index 2 in G, it only has two cosets in G. One of these is H and, because $b \notin H$, the other must be bH. Each element of G must be in H or bH so must be of the form a^i or of the form ba^i for some integer i with $0 \leq i < n$.

Because $bab^{-1} = a^{n-1}$ and $b^{-1} = b$, we have that $ab = ba^{n-1}$. As for the dihedral group, we can use the formula $ab = ba^{n-1}$ to express the product of any two elements of G in one of the forms a^i or a^ib.

It follows that the bijection $\phi : G \to D_n$ given by

Check that ϕ is a bijection.

$$\phi(a^i) = r^i \quad \text{and} \quad \phi(a^ib) = r^is$$

is an isomorphism. ■

Exercise 3.1

Let G be a group of order $2n$, where n is odd. Suppose that G has an element a of order n and an element b of order 2 and that $ab = ba$.

Show that the order of ab is $2n$.

Hint: use Lemma 2.7 of Chapter 6.

Theorem 3.4

If p is an odd prime, then every group of order $2p$ is isomorphic to either $\mathbb{Z}_{2p}$ or D_p.

Proof Let G be a non-cyclic group of order $2p$. By Cauchy's Theorem (Theorem 3.16 of Chapter 6), G has an element a of order p and an element b of order 2. Then $b \notin \langle a \rangle$ because its order, 2, is not a factor of $p = |\langle a \rangle|$.

By Lemma 3.3(a), we have $bab^{-1} = a^k$ where $0 < k < p$ and p divides $k^2 - 1 = (k+1)(k-1)$. As p is prime, either p divides $k+1$ or p divides $k-1$. Because $1 \leq k \leq p-1$, we have $p \geq k+1$ and so p cannot divide $k-1$. Thus the only possibilities are $k = p-1$ and $k = 1$.

If $k = 1$ then $ab = ba$, and so ab has order $2p$ by Exercise 3.1. In this case, $G = \langle ab \rangle \cong \mathbb{Z}_{2p}$ is cyclic.

If $k = p-1$, then Lemma 3.3(b) ensures that $G \cong D_p$. ■

Theorem 3.4 shows that all groups of order 6 are isomorphic to either $\mathbb{Z}_6$ or D_3, that all groups of order 10 are isomorphic to either $\mathbb{Z}_{10}$ or D_5, and that all groups of order 14 are isomorphic to either $\mathbb{Z}_{14}$ or D_7.

3.4 Groups of order 8

So far we have met five groups of order 8: the cyclic group $\mathbb{Z}_8$, the direct products $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, the dihedral group D_4 and the quaternion group Dic_2. We now find out whether there are any other possibilities.

Let G be a group of order 8. The possible orders of elements of G are 1, 2, 4 and 8. If $g \in G$ has order 4 or 8, then either g^2 or g^4 has order 2, so G has at least one element of order 2. Alternatively, Cauchy's Theorem gives the same conclusion. We now consider several cases.

Case 1

If G has an element g of order 8 then $G = \langle g \rangle$ is cyclic, that is,

$$G \cong \mathbb{Z}_8.$$

Case 2

Suppose that, apart from e, every element of G has order 2. Then every element of G is its own inverse and, for $a, b \in G$,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba;$$

hence G is abelian.

If $a \neq e$ and $b \notin \langle a \rangle$ then G contains a subgroup $H = \{e, a, b, ab\}$ that is isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let $K = \langle c \rangle$, where c is any of the four elements of $G \setminus H$. Then, by Proposition 1.9 of Chapter 6,

Recall that $G \setminus H = \{g \in G : g \notin H\}$.

$$G = HK \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Case 3

Suppose that G has an element a of order 4 and an element b of order 2 such that $b \notin \langle a \rangle$. By Lemma 3.3(a), we know that $bab^{-1} = a^j$ for some j such that $0 < j < 4$ and 4 divides $j^2 - 1$. The only possibilities are $j = 1$ and $j = 3$.

If $j = 3$ then $G \cong D_4$ by Lemma 3.3(b).

If $j = 1$ then $ba = ab$ and, setting $K = \langle b \rangle$ and applying Proposition 1.9 of Chapter 6, we get

$$G = HK \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

The above cases cover all the groups of order 8 listed at the beginning of the subsection, apart from Dic_2. The next proposition shows that the only group of order 8 missing from our initial list is indeed Dic_2.

Proposition 3.5

Let G be a group of order 8 that is not isomorphic to any of the groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and D_4. Then G has exactly one element d of order 2 and six elements

$$a^{\pm 1},\ b^{\pm 1} \text{ and } c^{\pm 1}$$

of order 4.

Moreover, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ and $ba = a^3b$.

Proof As $G \ncong \mathbb{Z}_8$, it has no element of order 8. Moreover, G must have at least one element, a say, of order 4, otherwise Case 2 would apply to give $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Let $d = a^2$ and let g be any element of order 2. Then $g \in \langle a \rangle$, otherwise we would have the situation of Case 3 and $G \cong D_4$ or $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

The only element of $\langle a \rangle$ of order 2 is d, so $g = d$. Hence the only element of G of order 2 is d and there are six elements of order 4, which must occur as three pairs of inverse elements, say $a^{\pm 1}$, $b^{\pm 1}$ and $c^{\pm 1}$.

Let $H = \langle a \rangle = \{e, a, a^2, a^3\}$. As H has index 2 in G, it only has two right cosets in G. One of these is H and, because $b \notin H$, the other must be

$$Hb = \{b, ab, a^2b, a^3b\}.$$

Since $G = H \cup Hb$, we get

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

as required. Notice that $d = a^2 = b^2$, $b^{-1} = b^3 = b^2b = db = a^2b$, and c must be either ab or a^3b.

Hence $(ab)^2 = d = a^2$, that is, $abab = a^2$. By cancellation,

$$bab = a$$

and so $ba = ab^{-1} = a^3b$. ■

Proposition 3.5 shows that, up to isomorphism, there is at most one group of order 8 not included in the three cases listed at the beginning of this subsection.

If such a group exists, then its elements satisfy the conditions in Proposition 3.5. But these conditions are precisely those we get from the standard form of the dicyclic group of order 8, Dic_2, introduced in Subsection 1.2. In particular, the elements satisfy the relations

$$a^4 = e = b^4,\ a^2 = b^2 (= d) \text{ and } ba = ab^{-1} = a^3b,$$

which is equivalent to $aba^3b = e$ (see Exercises 1.6 and 1.8). Hence such a group is again isomorphic to a group that we have already met.

Together with the case-by-case analysis that preceded it, Proposition 3.5 gives the following classification theorem for groups of order 8.

Theorem 3.6

Every group G of order 8 is isomorphic to one of the five groups

$$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_4,\ \mathrm{Dic}_2.$$

3.5 Groups of order 12

We now show that, up to isomorphism, there are five groups of order 12.

Exercise 3.2

Show that $D_3 \times \mathbb{Z}_2 \cong D_6$.

Exercise 3.3

Show that S_4 has only one subgroup of order 12.

Hint: use the sizes of conjugacy classes in S_4 and the fact that a subgroup of order 12 must be normal.

The next proposition gives a classification of *abelian* groups of order 12.

Proposition 3.7

Let G be an abelian group of order 12. Then either $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ or $G \cong \mathbb{Z}_{12}$.

Proof By Cauchy's Theorem, G has an element a of order 2 and an element b of order 3. Since $ab = ba$, the product ab has order 6, so $\langle ab \rangle$ is a normal subgroup and $\langle b \rangle$ is a subgroup of $\langle ab \rangle$.

Let $d \in G$ with $d \notin \langle ab \rangle$. We know that d has order 2, 3, 4, 6 or 12.

If d has order 2, then Proposition 1.9 in Chapter 6 gives

$$G = HK \cong \mathbb{Z}_6 \times \mathbb{Z}_2,$$

where $H = \langle ab \rangle$ and $K = \langle d \rangle$.

If d has order 3, then G has a subgroup $\langle b \rangle \times \langle d \rangle$ of order 9, which contradicts Lagrange's Theorem. Therefore this possibility does not arise.

If d has order 4, then bd has order 12, and $G = \langle bd \rangle$ is cyclic; that is,

$$G \cong \mathbb{Z}_{12}.$$

If d has order 12 then $G = \langle d \rangle \cong \mathbb{Z}_{12}$.

We are left with the possibility that all elements d of G that are not in $\langle ab \rangle$ have order 6. If d has order 6, then d^2 and d^3 have orders 3 and 2 respectively, and so they must be in $\langle ab \rangle$.

Hence

$$d = d^3 d^{-2} \in \langle ab \rangle,$$

contradicting the choice of d.

Thus if G is abelian of order 12, either $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ or $G \cong \mathbb{Z}_{12}$. ■

We are now left to find out what the *non*-abelian groups of order 12 are.

Proposition 3.8

Let G be a non-abelian group of order 12, and let a and b be elements of G such that:

(a) a has order 6

(b) b has order 2

(c) $b \notin \langle a \rangle$.

Then $G \cong D_6$.

Proof By Lemma 3.3(a), we know that

$$bab^{-1} = a^j$$

for some j such that $0 < j < 6$, and 6 divides $j^2 - 1$. The only possibilities are $j = 1$ and $j = 5$.

If $j = 1$, then $bab^{-1} = a$ gives $ba = ab$. Then

$$G = \langle a \rangle \langle b \rangle \cong \mathbb{Z}_6 \times \mathbb{Z}_2,$$

which is abelian.

Hence $j = 5$ and, by Lemma 3.3(b), $G \cong D_6$. ■

In the next result we are going to use the notion of the *kernel of a group action*. Let G be a group acting on a set X by an action $\wedge$, and let S_X denote the group of permutations of X. The action gives rise to a homomorphism $\phi : G \to S_X$, where the image of an element g of G is the permutation ϕ_g of X defined by

$$\phi_g(x) = g \wedge x \quad \text{for all } x \in X.$$

The defining properties of a group action ensure that ϕ is a homomorphism. The kernel of this homomorphism is called the **kernel of the action** $\wedge$ and it is denoted by $\ker \wedge$. An element g of G is in $\ker \wedge$ if ϕ_g is the identity permutation, so that

$$\ker \wedge = \{g \in G : g \wedge x = x \text{ for all } x \in X\}.$$

Thus $\ker \wedge$ is the set of those elements of G that stabilise *every* element of X. In particular, $\ker \wedge = \bigcap_{x \in X} \mathrm{Stab}(x)$.

Since $\ker \wedge$ is the kernel of a group homomorphism, it is a normal subgroup of G by Theorem 4.11 of Chapter 5.

Check for yourself that $\phi : G \to S_X$ is a group homomorphism.

Proposition 3.9

Let G be a group of order 12. Then:

(a) If G has a subgroup H of order 3 that is not normal, then $G \cong A_4$.

(b) If G has no element of order 6, then $G \cong A_4$.

Proof

(a) The group G acts on the set X of left cosets of H in G by

$$g \wedge aH = (ga)H.$$

Since the index of H in G is 4, the set X contains four elements. If we number these elements from 1 to 4, a permutation of X can be viewed as a permutation of the set $\{1, 2, 3, 4\}$, that is, as an element of S_4, and S_X is isomorphic to S_4.

The kernel K of this action is contained in $H = \mathrm{Stab}(H)$, and it is a normal subgroup of G. Since the order of H is prime, H has only two subgroups, namely H and $\{e\}$, and it is not itself normal in G. Therefore $K = \{e\}$.

We have observed that $S_X \cong S_4$, therefore ϕ can be viewed as a homomorphism from G to S_4 whose kernel is K. By the First Isomorphism Theorem, the group G is isomorphic to its image $\phi(G)$, which is isomorphic to a subgroup of S_4 of order 12.

We have seen from Exercise 3.3 that S_4 only has one subgroup of order 12, namely A_4. Therefore $\phi(G) = A_4$ and $G \cong A_4$.

(b) By Cauchy's Theorem, G has an element a of order 3.

Let $H = \langle a \rangle$ and suppose that H is normal. Then

$$bab^{-1} \in H = \{e, a, a^2\}$$

for all $b \in G$. The possibility $bab^{-1} = e$ cannot occur because $a \neq e$, so $bab^{-1} = a$ or a^2.

The centraliser $\mathrm{Cent}(a)$ of a in G is a subgroup of G containing H so, by Lagrange's Theorem, it has order 3, 6 or 12.

If it has order 6 or 12 then, by Cauchy's Theorem, it has an element g, say, of order 2. As $ag = ga$, the element ag would have order 6. As G has no such element, we must have $|\mathrm{Cent}(a)| = 3$ and hence

$$\mathrm{Cent}(a) = H.$$

Let $b, c \in G \setminus H$. Then $b \notin \mathrm{Cent}(a)$, so $ba \neq ab$ and hence $bab^{-1} \neq a$. Therefore $bab^{-1} = a^2$ and $ba = a^2b$. Similarly $ca = a^2c$.

Now consider bc. We have

$$bca = ba^2c = (ba)ac = a^2(ba)c = a^2a^2bc = a^4bc = abc,$$

thus $bc \in \mathrm{Cent}(a) = H$ for all $b, c \in G \setminus H$. But for each $b \in G \setminus H$, the nine different elements $c \in G \setminus H$ give rise, by the cancellation laws, to nine different elements bc. These cannot all be in H. Hence H cannot be normal and so, by part (a), $G \cong A_4$. ■

Proposition 3.10

Let G be a group of order 12 that is not isomorphic to any of the groups $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, D_6, A_4. Then G is not abelian, and it has an element b of order 6 such that every element of order 2 in G is in $\langle b \rangle$.

Moreover, G has two elements b and b^{-1} of order 6, two elements of order 3, one element $d = b^3$ of order 2, and six elements of order 4.

Proof Proposition 3.7 shows that G is not abelian. Proposition 3.9(b) shows that G has an element b of order 6, and Proposition 3.8 shows that every element of order 2 in G is in $\langle b \rangle$. So G has a unique element $d = b^3$ of order 2.

This is reminiscent of the situation in Proposition 3.5.

Let $H = \langle b \rangle$ and note that, in H:

- e has order 1
- b has order 6
- b^2 has order 3
- $b^3 = d$ has order 2
- b^4 has order 3
- $b^5 = b^{-1}$ has order 6.

We will show that the six elements of G not in H must all have order 4. To see this, let $a \in G$ with $a \notin H$. Then a cannot have order 2 because the only element of G of order 2 is in H. Moreover, G is not abelian, hence not cyclic, so no element has order 12. Therefore a has order 3, 4 or 6.

As H has index 2, it is normal in G, and H and aH are the only cosets of H in G. It follows that every element of G has one of the forms b^i or ab^i.

As G is not abelian, $ab \neq ba$, otherwise all pairs of elements commute. Since H is normal, $aba^{-1} \in H$ and, because $ab \neq ba$, we have $aba^{-1} \neq b$. Conjugation by a is an isomorphism by Proposition 2.1, so aba^{-1} has the same order as b and so it must be the other element of H of order 6, namely $aba^{-1} = b^5 = b^{-1}$. Note this also means that $ab^{-1}a^{-1} = (aba^{-1})^{-1} = (b^{-1})^{-1} = b$.

If a has order 3 or 6, then $a^3 = e$ or $a^3 = b^3 = d$, the unique element of order 2 in G. In both cases we have $a^3ba^{-3} = b$. However, we also have

$$a^3ba^{-3} = a^2b^{-1}a^{-2} = aba^{-1} = b^{-1}.$$

Hence it is impossible for a to have order 3 or 6 and a must have order 4.

To summarise, G has two elements b and b^{-1} of order 6, two elements of order 3, one element $d = b^3$ of order 2 and six elements of order 4, as required. ■

The next exercise shows that Dic_3 has the properties described in Proposition 3.10. Then Exercise 3.5 will give sufficient information to construct the Cayley table of any group of order 12 not covered by Propositions 3.7, 3.8 and 3.9, and shows that such a group must satisfy the conditions of Proposition 3.10. These two exercises complete the classification of groups of order 12.

Exercise 3.4

Show that the dicyclic group Dic_3 has two elements of order 6, two elements of order 3, one element of order 2 and six elements of order 4.

Exercise 3.5

Let G be any group of order 12 not isomorphic to any of the groups $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, D_6, A_4, so that the numbers of elements in G of orders $2, 3, 4$ and 6 are $1, 2, 6$ and 2 respectively.

Let a and b be elements of G with orders 4 and 6 respectively. Show that ab has order 4 and hence that $(ab)^2 = a^2$. Deduce that $ba = ab^{-1} = a^3b^2$, and hence show that $aba^3b = e$ and that G is Dic_3.

Hint: $a^2 = b^3$ is the unique element of order 2.

The propositions and exercises in this section give the following classification theorem for groups of order 12.

Theorem 3.11

Every group G of order 12 is isomorphic to one of the five groups

$$\mathbb{Z}_{12},\ \mathbb{Z}_6 \times \mathbb{Z}_2,\ A_4,\ D_6,\ \mathrm{Dic}_3.$$

Table 3.1 summarises the results we have obtained for groups of order up to and including 14.

Table 3.1 Groups of order up to and including 14

Order of group	Possible groups
1	$\mathbb{Z}_1 = \{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, $D_3 (\cong S_3)$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Dic_2
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, A_4, D_6, Dic_3
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7

4 Finite p-groups

This section investigates a particular class of groups: those whose order is a power of a prime. A key tool in the investigation is Theorem 2.14, which shows that if the quotient of a group by its centre is cyclic, then the group is abelian.

In this section, p will always denote a prime number.

4.1 p-groups and their subgroups

In Subsection 3.2 we saw that any group whose order is the square of a prime is abelian and isomorphic to a direct product of cyclic groups. This result does not generalise to groups whose order is any power of a prime, but we will see that this more general condition still has some important consequences for the structure of the group.

Definition 4.1 *Finite p-group*

Let p be a prime and n a positive integer. Then a group of order p^n is called a **p-group**.

In Theorem 2.15 we considered the case where $n = 2$ and we showed that groups of order p^2 are abelian.

While groups of order p^2 must be abelian, the situation is rather more complicated for groups of order p^3 – you need only consider the discussion

about groups of order 8 in Subsection 3.4 to realise this. This discussion produced three abelian and two non-abelian groups of order $2^3 = 8$. The non-abelian ones are the dihedral group D_4 and the dicyclic group Dic_2.

Theorem 2.13 tells us that the centre of a p-group must be non-trivial. This result does give *some* information about groups of order p^3: the centre $Z(G)$ of such a group G can only have order p, p^2 or p^3.

Exercise 4.1

Let G be a group of order p^3. Show that $Z(G)$ cannot have order p^2.

We have now reduced the possibilities for $|Z(G)|$ to p and p^3.

If the order of $Z(G)$ is p^3, the group G is abelian and Theorem 3.19 of Chapter 6 tells us that G is a direct product of cyclic groups, so G must be isomorphic to one of

$$\mathbb{Z}_{p^3}, \quad \mathbb{Z}_p \times \mathbb{Z}_{p^2} \quad \text{or} \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.$$

If the order of $Z(G)$ is p, then the quotient group $G/Z(G)$ has order p^2, so it is abelian by Theorem 2.15. It follows that $G/Z(G)$ may only be isomorphic to one of

$$\mathbb{Z}_{p^2} \quad \text{or} \quad \mathbb{Z}_p \times \mathbb{Z}_p.$$

However, if the quotient were $\mathbb{Z}_{p^2}$, we would have a cyclic quotient, so G would be abelian and the order of the centre would be p^3 and not p.

We conclude that a non-abelian group G of order p^3 has a centre of order p and that $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Unfortunately, this information does not uniquely determine the structure of G. For example, this discussion shows that any non-abelian group G of order 8 has a centre of order 2 and that the quotient by the centre is $\mathbb{Z}_2 \times \mathbb{Z}_2$. However, we know that there are two different non-abelian groups of order 8, and they must both satisfy these conditions.

This example shows that knowing the structure of a normal subgroup and the structure of the corresponding quotient group is not, in general, sufficient to determine the structure of the group itself.

It turns out that p-groups have an important structural property: a group of order p^n has a subgroup of order p^k for each positive $k \leq n$. In fact, a little more is true and the full result is contained in Theorem 4.3 below. First we give a lemma that is needed for the proof in the abelian case.

Lemma 4.2

Let G be an abelian p-group of order p^n for some positive integer n, with $n \geq 2$. Then G has a subgroup of order p^{n-1}.

Proof The proof is by induction on n.

If $n = 2$, by Cauchy's Theorem G has an element of order p, which generates a subgroup of order p.

Now assume that every abelian group of order p^k, where $k > 2$, has a subgroup of order p^{k-1}.

Suppose that G has order p^{k+1}. Then G has a subgroup H, say, of order p by Cauchy's Theorem. Since G is abelian, H is normal in G. The quotient group G/H is abelian and it has order

$$\frac{|G|}{|H|} = p^k.$$

By the induction hypothesis, G/H has a subgroup of order p^{k-1}. By the Correspondence Theorem (Theorem 4.17 of Chapter 5), we know this subgroup must have the form K/H for some subgroup K of G. But now

$$|K/H| = \frac{|K|}{|H|} = \frac{|K|}{p} = p^{k-1},$$

which implies that K has order p^k. ■

Theorem 4.3

Let G be a p-group of order p^n for some positive integer n. Then there exist normal subgroups

$$\{e\} = H_0, H_1, \ldots, H_n = G$$

of G such that

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G,$$

where $|H_i| = p^i$ for $i = 0, \ldots, n$.

Because of the set inclusions involving the H_i, we say that the H_i form a *chain* of subgroups.

Proof The proof is by induction on n.

For $n = 1$, the order of G is p and the required chain is simply

$$\{e\} = H_0 \subset H_1 = G.$$

We have $|H_i| = p^i$ for $i = 0, 1$ and the normality condition is trivially true.

Now assume that the theorem is true for all groups of order p^r, where $r \leq k$, and let G have order p^{k+1}.

If G is abelian, then, since p^k divides p^{k+1}, G has a subgroup H_k of order p^k by Lemma 4.2. By the induction hypothesis, H_k has a chain of subgroups with the correct orders:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{k-1} \subset H_k.$$

Combining this with $H_k \subset H_{k+1} = G$, we obtain the required chain:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_k \subset H_{k+1} = G.$$

Since G is abelian, normality is automatic.

Now we consider the case where G is *not* abelian. Our strategy is to use what we know about the centre of a p-group to construct the chain of subgroups in two stages: from the trivial subgroup to the centre and then from the centre to the whole group.

Since G is non-abelian, its centre $Z(G)$ is not the whole group and so its order is *less* than p^{k+1}. By Lagrange's Theorem, $Z(G)$ is a p-group. So $|Z(G)| = p^s$, where $0 \leq s \leq k$, and we may apply the induction hypothesis to $Z(G)$.

Thus, there exists a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = Z(G)$$

of $Z(G)$ where $|H_i| = p^i$ for $i = 0, \ldots, s$. These subgroups are also subgroups of G. Furthermore, by Exercise 2.5, they are normal subgroups of G.

We now have the part of the required chain from the trivial subgroup to $Z(G)$, and we turn to completing the chain from $Z(G)$ to G.

To apply the induction hypothesis, we need another p-group of order less than p^{k+1}. The one we will use is the quotient of G by its centre.

Since G is a p-group, Theorem 2.13 tells us that $Z(G)$ has at least p elements. Hence

$$|Z(G)| = p^s, \quad 1 \leq s.$$

Since $Z(G)$ is normal in G, we may consider the quotient group $G/Z(G)$, whose order is

$$p^{k+1}/p^s = p^{k+1-s} \leq p^k.$$

Hence the quotient is a p-group to which we may apply the induction hypothesis. It follows that there exists a chain of normal subgroups of the quotient,

$$\{Z(G)\} = K_0 \subset K_1 \subset \cdots \subset K_{k+1-s} = G/Z(G),$$

where $|K_i| = p^i$, $i = 0, \ldots, k+1-s$.

To complete the proof, we must show that the chain of normal subgroups in the quotient group $G/Z(G)$ may be used to define a chain of normal subgroups of G between $Z(G)$ and G. The fact that we can do so is an immediate consequence of the Correspondence Theorem (Theorem 4.17 of Chapter 5), which tells us that each normal subgroup K_i of $G/Z(G)$ gives rise to a normal subgroup H_{i+s} of G that contains $Z(G)$. Since the correspondence is one–one and the K_is are all distinct, so are the H_{i+s}s. Moreover, the trivial subgroup K_0 of the quotient group corresponds to $Z(G) = H_s$.

The proof of the Correspondence Theorem shows that set inclusion is preserved by the correspondence. Hence we have a chain of normal subgroups

$$Z(G) = H_s \subset H_{s+1} \subset \cdots \subset H_{k+1} = G.$$

We know that $|Z(G)| = p^s$ and $|G| = p^{k+1}$, and also that there are $k - s$ subgroups in the (strictly inclusive) chain *between* $H_s = Z(G)$ and $H_{k+1} = G$, each of order p^i for some i. Therefore we must have $|H_i| = p^i$ for $i = s, \ldots, k+1$.

We have now constructed a chain of normal subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = Z(G) = H_s \subset \cdots \subset H_{k+1} = G$$

for G, where $|H_i| = p^i$, $i = 0, \ldots, k+1$, completing the inductive step. ■

4.2 Soluble groups

We have just shown that finite p-groups have a chain of normal subgroups, each contained in the next. Under certain conditions, a chain of subgroups satisfying some additional requirements is enough to pin down a group up to isomorphism. Thus, finding chains of subgroups with given properties is another approach to classifying groups.

In order to get useful information about a group G, often it is enough to require that each subgroup in the chain is normal in its successor, rather than in the whole of G. In any case, the key idea is to make the chain as long as possible. This is achieved by requiring the quotient groups formed from successive subgroups to be, in some sense, as small as possible. A suitable sense of 'small' for these quotients is that they should have no non-trivial normal subgroup, because otherwise the chain can be extended using the Correspondence Theorem – you will see this in Exercise 4.2.

We first name groups that give rise to small quotients in this sense.

Definition 4.4 *Simple group*

A group G with more than one element is said to be a **simple group** if it has no non-trivial proper normal subgroups.

In the following exercise, you are asked to work with a chain of subgroups each of which is normal in its successor.

Exercise 4.2

Let G be a group with a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = G,$$

where H_i is a normal subgroup of H_{i+1} for $i \in \{0, \ldots, n-1\}$.

Suppose that K is a proper non-trivial normal subgroup of H_{i+1}/H_i. Show that the chain of subgroups can be extended to

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset J \subset H_{i+1} \subset \cdots \subset H_s = G,$$

where the inclusions are all proper (that is, $H_i \subsetneq H_{i+1}$).

The aim of the next exercise is to show that A_5 is a simple group.

Exercise 4.3

(a) Write down the cycle types of elements of A_5 together with the number of elements of each type.

(b) Use the list in part (a) to divide A_5 into conjugacy classes, remembering that some of the cycle types may split into more than one conjugacy class in A_5 if the conjugating elements in S_5 are odd permutations.

(c) Deduce that A_5 is a simple group.

We now give a description of a chain of subgroups that all finite groups possess.

Definition 4.5 *Composition series*

Let G be a group and suppose that $\{e\} = H_0, H_1, \ldots, H_n = G$ are subgroups of G such that:

(a) $\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G$

(b) H_i is a normal subgroup of H_{i+1} for $i = 1, \ldots, n-1$

(c) H_{i+1}/H_i is a simple group for $i = 0, \ldots, n-1$.

Then we say that $H_0, H_1, \ldots, H_n$ are a **composition series** for G of **length** n.

Example 4.6 *Composition series for S_3 and S_4*

$\{e\} \subset A_3 \subset S_3$ is a composition series for S_3.

$\{e\} \subset \{e, (12)(34)\} \subset V \subset A_4 \subset S_4$ is a composition series for S_4, where V is the Klein group regarded as a subgroup of S_4, that is $V = \{e, (12)(34), (13)(24), (14)(23)\}$.

It is not hard to see that every finite group has a composition series: starting with the group G, identify a maximal normal subgroup N (and remember that such a subgroup always exists, because $\{e\}$ is normal in any group). Maximality ensures that the quotient group is simple. Continue in this way until $\{e\}$ is reached.

An important result that makes composition series a relevant tool for classification is the Jordan–Hölder Theorem. This says that any two composition series of the same group have the same length, and that the quotient groups in each series can be put into one–one correspondence with matching pairs being isomorphic.

For example, the dihedral group D_4 has two normal subgroups of order 4: the group of rotations $R = \langle r \rangle$ and the Klein group V. The subgroup $\{e, r^2\}$ is contained in both R and V, so D_4 has two composition series:

$$\{e\} \subset \langle r^2 \rangle \subset R \subset D_4 \quad \text{and}$$
$$\{e\} \subset \langle r^2 \rangle \subset V \subset D_4.$$

Although these two series are different, they have the same length and all the quotient groups are cyclic and of order 2, so they are isomorphic.

Since groups of prime order are cyclic and necessarily simple, groups where the quotient groups in the composition series have prime order are of particular interest.

Definition 4.7 *Soluble group*

Let G be a group and suppose that G has subgroups $\{e\} = H_0, H_1, \ldots, H_n = G$ such that

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G,$$

where H_i is a normal subgroup of H_{i+1} and H_{i+1}/H_i is a cyclic group of prime order for $i = 0, \ldots, n-1$.

Then G is said to be a **soluble group**.

Thus, finite p-groups are soluble by Theorem 4.3. A key example of a group that is not soluble is S_5. This is because A_5 is simple, thus a composition series for S_5 is

$$\{e\} \subset A_5 \subset S_5,$$

and the quotient $A_5/\{e\}$ is simple but not of prime order.

There is a famous branch of mathematics, known as Galois Theory, that uses group theory to obtain results about the solvability of polynomial equations *by radicals*.

A *polynomial equation* of *degree* n is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_n \neq 0$$

where the a_i are real numbers, or complex numbers, or elements of more general algebraic structures. You have met polynomial equations with real coefficients in your previous studies. For example, quadratic equations such as

$$4x^2 + 3x - 17 = 0$$

are polynomial equations of degree 2.

The phrase 'solving by radicals' means solving an equation through a process that combines standard arithmetic operations with taking successive roots. The familiar formula that says that the solutions of the quadratic equation

$$ax^2 + bx + c = 0, \text{ for } a \neq 0$$

are given by $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ is an example of a solution by radicals.

Galois Theory associates a subgroup of the symmetric group S_n to a polynomial equation of degree n. It turns out that the subgroup is soluble if, and only if, the equation can be solved by radicals. Unfortunately, here we do not have space to discuss any of the details of this association, but you will be in a good position to read further on the subject when you have completed this module.

Since S_2, S_3 and S_4 are all soluble groups, the association that we have just described can be used to show that polynomial equations of degree up to 4 can always be solved by radicals. Indeed, algorithms for such solutions were in existence long before Galois Theory was developed, although those for degree 3 and 4 came a long time after the formula to solve quadratic equations.

However, as S_5 is not soluble, and neither is S_n for $n > 5$, any polynomial equation whose associated group is the whole of S_5, or indeed S_n for $n > 5$, cannot be solved by radicals.

This is a very powerful result: it means that for polynomial equations of degree greater than or equal to 5, we cannot hope to find a general formula that will give us the solutions in terms of a finite number of additions, subtractions, multiplications, divisions and root extractions of the coefficients.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Express products of elements of a group defined by generators and relations in an appropriate standard form.

(b) Recognise the dihedral and dicyclic groups when described using a standard form.

(c) Find subgroups generated by finite sets in simple cases.

(d) Find centres and centralisers of groups in simple cases.

(e) Find the class equation of groups of small order, including S_n.

(f) Apply the type of argument used to classify groups of order up to 14.

(g) Find the composition series of a group in simple cases.

(h) Construct proofs, similar to those in the chapter, based on the group axioms and the results of the chapter.

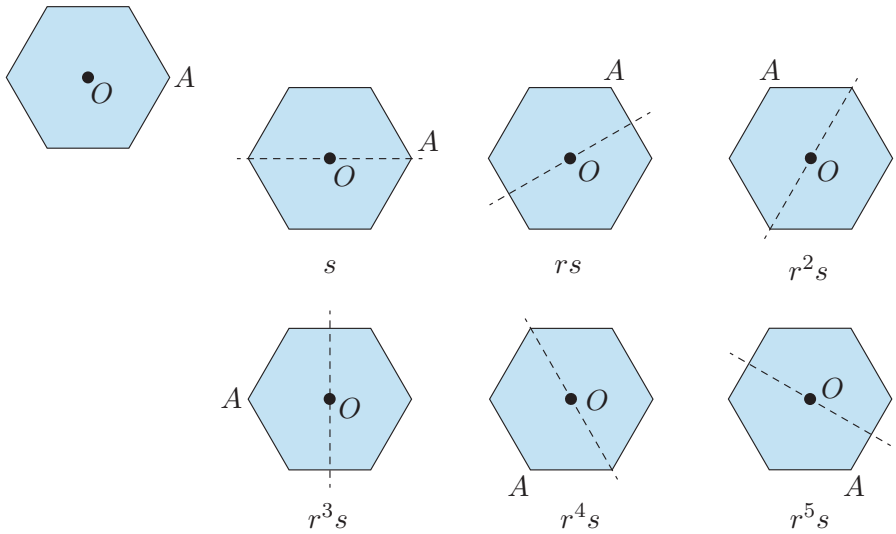
Solutions to exercises

Solution to Exercise 1.1

(a) All the rotations in D_6 are obtained by repeating r a sufficient number of times. Thus the rotations are

$$r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6 = r^0 = e.$$

(b) The easiest way to find out which reflection corresponds to each expression of the form $r^n s$ is to keep track of what happens to the vertices of the hexagon under each composite transformation. These transformations are illustrated in the figure below.



(c) By inspection, we find that $sr = r^5 s$.

You may have expressed this element in the form $r^{-1}s$, which is the same because $r^{-1} = r^5$.

Solution to Exercise 1.2

(a) $sr^2 = srr = r^5 sr = r^5 r^5 s = r^{10} s = r^4 s$

$sr^3 = sr^2 r = r^4 sr = r^4 r^5 s = r^9 s = r^3 s$

The second result should be no surprise as r^3 is rotation through π and so commutes with all the elements of D_6. If you spotted this and used it in your solution, well done!

(b) $s^5 = s$

Solution to Exercise 1.3

(a) This is the cyclic group $\mathbb{Z}_6$.

(b) This is the dihedral group D_4 – the symmetry group of a square.

(c) This is the Klein group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The relation $sr = rs$ means that the two generators commute. A little thought might convince you that this implies the group is abelian. In addition, the standard form shows the group has four elements, and it is not hard to see that no element has order greater than 2. These conditions are enough to show that the group is isomorphic to V.

Solution to Exercise 1.4

(a) Firstly we show that N is a subgroup of G.

Closure The only non-trivial product to check is $r^2r^2 = e$. So N satisfies the closure axiom.

Identity As e is in N, the identity axiom is satisfied.

Inverses As $e^{-1} = e$ and $\left(r^2\right)^{-1} = r^2$, the inverses axiom is satisfied.

Hence N is a subgroup of G.

Alternatively, simply note that $N = \langle r^2 \rangle$.

Next, we must show that N is normal. By Proposition 3.7 of Chapter 5, we need to check that aNa^{-1} is a subset of N for each a in G.

As $aea^{-1} = e \in N$ for each a in G, we only have to check that ar^2a^{-1} is in N. Using the relations $r^4 = s^2 = e$ and $sr = r^3s$ gives the following.

$$\begin{aligned}
er^2e^{-1} &= r^2 \\
rr^2r^{-1} &= r^2 \\
(r^2)r^2(r^2)^{-1} &= r^2 \\
(r^3)r^2(r^3)^{-1} &= r^2 \\
sr^2s^{-1} &= r^2 \\
(rs)r^2(rs)^{-1} &= r^2 \\
(r^2s)r^2(r^2s)^{-1} &= r^2 \\
(r^3s)r^2(r^3s)^{-1} &= r^2
\end{aligned}$$

This completes the proof that N is a normal subgroup of G.

(b) The distinct left cosets of $N = \{e, r^2\}$ are

$$\begin{aligned}
eN &= r^2N = N, \\
rN &= r^3N = \{r, r^3\}, \\
sN &= r^2sN = \{s, r^2s\}, \\
rsN &= r^3sN = \{rs, r^3s\}.
\end{aligned}$$

(c) The Cayley table of G/N is as follows.

$\circ$	N	rN	sN	rsN
N	N	rN	sN	rsN
rN	rN	N	rsN	sN
sN	sN	rsN	N	rN
rsN	rsN	sN	rN	N

Solution to Exercise 1.5

(a) $\overline{K}_1 = \{N, rsN\}$, $\overline{K}_2 = \{N, r^2sN\}$.

(b) $K_1 = \{e, r^3, rs, r^4s\}$, $K_2 = \{e, r^3, r^2s, r^5s\}$.

Solution to Exercise 1.6

(a) $b^4 = (b^2)^2 = a^4 = e$

(b) $b^2a = a^2a = a^3 = aa^2 = ab^2$ and $b^2b = b^3 = bb^2$

(c)
$$\begin{aligned} aba^3b = e &\Rightarrow aaba^3b = a \\ &\Rightarrow ba^2ba^3b = ba \\ &\Rightarrow b^4a^3b = ba && \text{using } a^2 = b^2 \\ &\Rightarrow a^3b = ba && \text{using } a^4 = e \text{ and } a^2 = b^2 \end{aligned}$$

(d) The result in part (c) means that in any word involving a and b we can successively move all the bs to the right. This will give us a word of the form $\alpha\beta$, where α is a word containing only as and β is a word containing only bs.

We can then use $a^4 = e$ and $b^4 = e$ to reduce α and β to a^r and b^s respectively for some $r, s \in \{0, 1, 2, 3\}$.

Lastly, we can use $b^2 = a^2$ and $b^3 = a^2b$ to write an element g of Dic_2 in the form $g = a^rb^s : \ r = 0, \ldots, 3, \ s = 0, 1$.

Solution to Exercise 1.7

(a) We have

$$a^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and}$$

$$b^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

so $a^2 = b^2$. Moreover, $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, that is, $(a^2)^2 = a^4 = e$.

Another matrix calculation shows that $aba^3b = e$.

Calculation also shows that the eight matrices

$$a^rb^s : \ r = 0, \ldots, 3, \ s = 0, 1$$

are distinct, and the required result follows.

(b) Both $\langle a \rangle$ and $\langle b \rangle$ are cyclic subgroups of order 4. Moreover, the product $ab = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$ also generates a cyclic subgroup of order 4. Since $|G| = 8$, these three subgroups of order 4 have index 2 in G, and so they are normal.

Solution to Exercise 1.8

Since $a^4 = e$, we have $a^3 = a^{-1}$.

Since $a^2 = b^n$ and $a^4 = e$, we have $a^4 = (b^n)^2 = b^{2n} = e$, hence

$$b^{2n-1} = b^{-1}.$$

Now $aba^3b = e \Rightarrow ba^3b = a^{-1} = a^3$
$\Rightarrow ba^3 = a^3b^{-1} = a^3b^{2n-1}$
$\Rightarrow ba^3 = a^3a^2b^{n-1} = ab^{n-1}$
$\Rightarrow ba = ab^{n-1}a^2 = a^3b^{n-1}$.

We can use this relation to rewrite any word in a, b as a word in a followed by a word in b, that is, a power of a followed by a power of b. We then use

$$a^4 = e, \quad a^2 = b^n$$

to ensure that the power of a is one of $a^0(= e), a, a^2, a^3$ and the power of b is one of $b^0(= e), b, \ldots, b^{n-1}$.

This shows that every element of Dic_n can be written in the required form. Since this form gives $4n$ elements and Dic_n has order $4n$, we have a standard form.

Solution to Exercise 1.9

Let $H = \langle S \rangle$. Since $(1\,2\,3) = (1\,2)(2\,3)$, it is clear that $H \subseteq A_4$.

Now $a = (1\,2\,3)$ has order 3 and $b = (1\,2)(3\,4)$ has order 2, so H has order at least 6. Since $|A_4| = 12$, either $|H| = 6$ or $|H| = 12$. We have that

$$ab = (1\,2\,3)(1\,2)(3\,4) = (1\,3\,4),$$
$$a^2b = (1\,3\,2)(1\,2)(3\,4) = (2\,3\,4),$$
$$ba = (1\,2)(3\,4)(1\,2\,3) = (2\,4\,3).$$

It follows that $\{e, a, a^2, b, ab, a^2b, ba\} \subseteq H$, so H contains at least seven distinct elements of A_4. Therefore we must have $|H| = 12$, hence $H = A_4$ as required.

Solution to Exercise 1.10

We have $b^{-1} = b$, so

$$bab^{-1} = (2\,5)(3\,4)(1\,2\,3\,4\,5)(2\,5)(3\,4) = (1\,5\,4\,3\,2).$$

Since $(1\,5\,4\,3\,2) = a^{-1}$ and a has order 5, we can deduce

$$bab^{-1} = a^{-1} = a^4,$$

hence $ba = a^4b$. By Proposition 1.7 we know that

$$H = \{s_1^{r_1} \cdots s_n^{r_n} : n \in \mathbb{N}, s_i \in \{a, b\}, r_i \in \mathbb{Z}, i = 1, \ldots, n\}.$$

Since $ba = a^4b$ we can successively swap terms in any expression $s_1^{r_1} \cdots s_n^{r_n}$ so that the expression can be written as $a^r b^s$. Since $a^5 = b^2 = e$, we have that $H = \{a^r b^s : r = 0, \ldots, 4, s = 0, 1\}$. This set contains at most ten elements. Note that we have to say 'at most' since we cannot be sure that these elements are distinct.

The order of a is 5 and that of b is 2. Hence by Proposition 4.5 of Chapter 5, both 5 and 2 divide the order of H. Therefore $|H|$ is a multiple of 10, and hence at least 10.

Thus we have shown that the order of H is 10, as required.

Solution to Exercise 2.1

(a) $srs^{-1} = r^4$ and $rsr^{-1} = rsr^4 = r^2s$ in D_5.

(b) $srs^{-1} = r^5$ and $rsr^{-1} = rsr^5 = r^2s$ in D_6.

Solution to Exercise 2.2

To find a conjugacy class $\mathrm{Conj}_G(a)$, we compute the conjugates gag^{-1} and use some ingenuity to reduce the number of calculations. Proposition 2.5 is useful. In particular:

- a is conjugate to b if, and only if, $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$
- all the elements of a conjugacy class have the same order
- $|\mathrm{Conj}_G(a)|$ divides $|G|$ whenever G is a finite group.

(a) In D_4, the relation $sr = r^3s$ is equivalent to the more general relation $sr = r^{-1}s$, which holds in *any* dihedral group. From this we get $sr^{-1} = rs$, and repeatedly multiplying on the left by r and simplifying gives the useful relation

$$sr^{-i} = r^i s,$$

which holds in *any* dihedral group.

In D_4, taking $i = 2$ gives

$$sr^{-2} = sr^2 = r^2 s,$$

which means that r^2 commutes with s. Since r^2 also commutes with every element of the form r^i, it commutes with every element of D_4.

We therefore have two single-element conjugacy classes, $\{e\}$ and $\{r^2\}$.

Now consider the element r. First we try conjugating r by s (this makes the calculations easy). We get

$$srs^{-1} = r^{-1}ss^{-1} = r^{-1} = r^3,$$

so $r^3 \in \mathrm{Conj}(r)$. There are no other elements of order 4 in D_4, so $\{r, r^3\}$ is the whole of $\mathrm{Conj}(r)$.

Now consider the elements s and rs. First we try conjugating s by r and rs by r^{-1} (again to make the calculations easy). We get

$$rsr^{-1} = rrs = r^2 s$$

and

$$r^{-1}(rs)r = sr = r^3 s.$$

These elements form either two conjugacy classes, $\{s, r^2 s\}$ and $\{rs, r^3 s\}$, or a single one, $\{s, r^2 s, rs, r^3 s\}$. To determine which occurs, we calculate all the conjugates of s. Conjugating

- by an element of the form r^i (a rotation) gives $r^i s r^{-i} = r^i r^i s = r^{2i} s$
- by an element of the form $r^i s$ (a reflection) gives $r^i s s (r^i s)^{-1} = r^i s s r^i s = r^i r^i s = r^{2i} s$.

Thus, s is conjugate to $r^2 s$ but not to rs or $r^3 s$. The conjugacy classes are

$$\{e\}, \{r^2\}, \{r, r^3\}, \{s, r^2 s\} \text{ and } \{rs, r^3 s\}.$$

Therefore the class equation is $8 = 1 + 1 + 2 + 2 + 2$.

(b) By Exercise 1.8, in *any* dicyclic group Dic_n, we have

$$b^{-1} = b^{2n-1} = a^2 b^{n-1}$$

and

$$ba = a^3 b^{n-1} = ab^{-1}.$$

In Dic_2 these equalities become $b^{-1} = a^2 b$ and $ba = a^3 b = ab^{-1}$.

Now, $a^2 = b^2$, which means that a^2 commutes with b. Since a^2 also commutes with every element of the form a^i, it commutes with every element in Dic_2.

We therefore have two single-element conjugacy classes, $\{e\}$ and $\{a^2\}$.

To find the other conjugacy classes, we start by finding some specific conjugates. We try to choose conjugating elements that make the calculations as easy as possible.

First consider the element a: we have $bab^{-1} = a^3 bb^{-1} = a^3$, which gives $\{a, a^3\} \subseteq \mathrm{Conj}(a)$.

Now consider the element b: we have $a^{-1}ba = a^{-1}a^3 b = a^2 b$, which gives $\{b, a^2 b\} \subseteq \mathrm{Conj}(b)$.

Now consider the element ab: we have $b(ab)b^{-1} = ba = a^3 b$, which gives $\{ab, a^3 b\} \subseteq \mathrm{Conj}(ab)$.

Since the size of a conjugacy class divides the order of the group, these sets form either three disjoint conjugacy classes, or one conjugacy class of four elements and one of two. Unfortunately, we need some further calculation to determine which case occurs.

First we calculate all the conjugates of a:

$$a^i a a^{-i} = a \quad \text{and} \quad a^i ba(a^i b)^{-1} = a^i bab^{-1}a^{-i} = a^i a^3 a^{-i} = a^3,$$

so one conjugacy class is $\{a, a^3\}$.

Next we calculate all the conjugates of b (noting that a^{-i} is easier than a^i):

$$a^{-i}ba^i = a^{-i}a^3ba^{i-1} = \cdots = a^{-i}a^{3i}b = a^{2i}b$$

and

$$(a^ib)^{-1}b(a^ib) = b^{-1}(a^{-i}ba^i)b = b^{-1}(a^{2i}b)b = a^{2i}b^{-1}b^2 = a^{2i}b,$$

so another conjugacy class is $\{b, a^2b\}$. The final class is $\{ab, a^3b\}$.

The conjugacy classes are

$$\{e\}, \{a^2\}, \{a, a^3\}, \{ab, a^3b\}, \{b, a^2b\}.$$

Hence the class equation is $8 = 1 + 1 + 2 + 2 + 2$.

Solution to Exercise 2.3

(a) $\mathrm{Cent}_{S_3}(1\,2\,3) = \{e, (1\,2\,3), (1\,3\,2)\} = \langle(1\,2\,3)\rangle$, since $(1\,2)$ does not commute with $(1\,2\,3)$ and so the centraliser cannot be the whole group.

$\mathrm{Cent}_{S_3}(1\,2) = \{e, (1\,2)\} = \langle(1\,2)\rangle$, since $(1\,2\,3)$ does not commute with $(1\,2)$, and so the centraliser cannot be the whole group.

(b) $\mathrm{Cent}_{D_4}(r^2) = D_4$, since r^2 commutes with all the elements of D_4. So $\langle r^2\rangle \neq \mathrm{Cent}_{D_4}(r^2)$.

Since s and e commute with s, and so does r^2 (which in fact commutes with every element of D_4), we must have $\{e, s, r^2\} \subseteq \mathrm{Cent}_{D_4}(s)$. Since $\mathrm{Cent}_{D_4}(s)$ is a subgroup of D_4, we must have $r^2s \in \mathrm{Cent}_{D_4}(s)$. Moreover, r does not commute with s, so this centraliser cannot be the whole group. Therefore $\mathrm{Cent}_{D_4}(s) = \{e, s, r^2, r^2s\}$ and $\mathrm{Cent}_{D_4}(s) \neq \langle s\rangle$.

Solution to Exercise 2.4

(a) The centraliser of any element is the whole group.

(b) In any group G, we have $\mathrm{Cent}_G(e_G) = G$.

Solution to Exercise 2.5

Since H is a subgroup of $Z(G)$, it is also a subgroup of G and so we only need to show that H is normal in G.

As in the proof of Proposition 2.9, let $a \in H$ and $g \in G$. Then, since a is a central element of G, we have $gag^{-1} = a \in H$, so that H is a normal subgroup of G by Proposition 3.7 of Chapter 5.

Solution to Exercise 2.6

(a) $\mathrm{Cent}_{S_3}(1\,3) = \{e, (1\,3)\}$

(b) An element of the centre commutes with every other element, so in particular with $(1\,3)$. This gives $Z(S_3) \subseteq \mathrm{Cent}_{S_3}(1\,3)$. We know that $(1\,3)$ is not in the centre, for otherwise $\mathrm{Cent}_{S_3}(1\,3)$ would be the whole of S_3, so we have $Z(S_3) = \{e\}$.

Solution to Exercise 2.7

(a) $Z(\mathrm{Dic}_2) = \{e, a^2\}$.

(b) $\mathrm{Conj}_{\mathrm{Dic}_2}(a) = \{a, a^3\}$.

(c) The elements a^i all commute with a, so $\{e, a, a^2, a^3\} \subseteq \mathrm{Cent}_{\mathrm{Dic}_2}(a)$.

By Theorem 2.11,

$$|\mathrm{Cent}_{\mathrm{Dic}_2}(a)| = |G|/|\mathrm{Conj}_{\mathrm{Dic}_2}(a)| = \tfrac{8}{4} = 4.$$

Hence $\mathrm{Cent}_{\mathrm{Dic}_2}(a) = \{e, a, a^2, a^3\}$.

Solution to Exercise 3.1

Since a has order n, we have $|\langle a\rangle| = n$. Therefore $b \notin \langle a\rangle$, as the order of b is 2 and 2 does not divide n. Now $\langle b\rangle = \{e, b\}$, and so $\langle a\rangle \cap \langle b\rangle = \{e\}$. Therefore, by Lemma 2.7 of Chapter 6, the order of ab is $\mathrm{lcm}(2, n) = 2n$, as required.

Solution to Exercise 3.2

Recall that

$$D_6 = \{r^m s^n : m = 0, \ldots, 5, n = 0, 1; r^6 = s^2 = e, sr = r^5 s\}.$$

Let H be the subgroup of D_6 generated by r^2 and s, and let K be the subgroup generated by r^3. Then

$$H = \{e, r^2, r^4, s, r^2 s, r^4 s\} \quad \text{and} \quad K = \{e, r^3\},$$

so $H \cong D_3$ and $K \cong \mathbb{Z}_2$.

Moreover, H and K are both normal in D_6: H because it has index 2, and K because r^3 is central. Now every element of D_6 can be written in the form kh with $k \in K$ and $h \in H$, and $K \cap H = \{e\}$. Thus, by Proposition 1.9 of Chapter 6,

$$D_6 \cong K \times H \cong H \times K,$$

therefore $D_6 \cong D_3 \times \mathbb{Z}_2$, as required.

Solution to Exercise 3.3

From Exercise 5.5 of Chapter 5, we know that S_4 has five conjugacy classes, namely:

- $\{e\}$, of size 1
- the set containing the 4-cycles, of size 6
- the set containing products of 2-cycles, of size 3
- the set containing the 3-cycles, of size 8
- the set containing the 2-cycles, of size 6.

Since a subgroup of S_4 of size 12 is necessarily normal, it must be a union of conjugacy classes by Proposition 3.12 of Chapter 5. Moreover, any subgroup contains the identity, hence the conjugacy class of size 1. Therefore any subgroup of order 12 must contain the three pairs of 2-cycles, otherwise the order of the subgroup would be an odd number.

Then the only way to obtain 12 elements as a union of conjugacy classes is to include the eight 3-cycles. This gives A_4, as required.

Solution to Exercise 3.4

We know that

$$\mathrm{Dic}_3 = \{a^r b^s : r = 0, \ldots, 3,\ s = 0, \ldots, 2; a^4 = e, a^2 = b^3, aba^3b = e\},$$

and $ba = a^3b^2 = ab^{-1}$ (see Exercise 1.8).

Then:

- b and $b^5 = a^2b^2$ have order 6
- b^2 and $b^4 = a^2b$ have order 3
- $a^2 = b^3$ has order 2
- $a, a^3, ab, a^3b, ab^2, a^3b^2$ all have order 4.

To see that ab, a^3b, ab^2 and a^3b^2 all have order 4, note that ab and a^3b are inverse to each other, and so they have the same order. To check that their order is 4, note that

$$abab = a(ab^{-1})b = a^2.$$

Likewise, ab^2 and a^3b^2 are inverse to each other and

$$ab^2ab^2 = abab^{-1}b^2 = abab\,,$$

so these two elements also have order 4.

Solution to Exercise 3.5

Since b has order 6, we have that b and $b^5 = b^{-1}$ are the two elements of order 6 and that b^2 and b^4 are the two elements of order 3.

Since a has order 4, a^2 has order 2. Similarly, b^3 has order 2. Since G has a unique element of order 2, we have that $a^2 = b^3$.

The element ab cannot be the unique element of order 2, otherwise $ab = a^2$, which implies $b = a$, contradicting the fact that a and b have different orders. The element ab cannot have order 3, because otherwise either $ab = b^2$ or $ab = b^4$, either of which gives a contradiction, as above.

Finally, the element ab cannot have order 6, because otherwise either $ab = b$ or $ab = b^5$, either of which gives a contradiction. The only remaining possibility is that ab has order 4. This means that $(ab)^2$ has order 2 and hence that $(ab)^2 = a^2$.

Now, $abab = a^2$ implies that $bab = a$ and hence that

$$ba = ab^{-1} = ab^5 = a^3b^2.$$

Finally, $aba^3b = ab(a^3b^2)b^{-1} = abbab^{-1} = ab^2ba = ab^3a = aa^2a = a^4 = e$.

Hence G satisfies all the relations $a^4 = e$, $a^2 = b^3$ and $aba^3b = e$, and therefore G is Dic_3.

Solution to Exercise 4.1

If $Z(G)$ has order p^2, then the quotient group $G/Z(G)$ has order p and is therefore cyclic. Then, by Theorem 2.14, G is abelian, which implies that $Z(G) = G$ has order p^3, a contradiction. Thus $Z(G)$ cannot have order p^2.

Solution to Exercise 4.2

Since K is a proper non-trivial normal subgroup of H_{i+1}/H_i, by the Correspondence Theorem there is a proper normal subgroup J of H_{i+1} that properly contains H_i. The chain can therefore be extended to

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset J \subset H_{i+1} \subset \cdots \subset H_s = G.$$

Solution to Exercise 4.3

(a)

Cycle type	Number of elements
(1)(2)(3)(4)(5)	1
(--)(--)	15
(---)	20
(-----)	24

(b)

Representative of conjugacy class	Size of conjugacy class
(1)(2)(3)(4)(5)	1
(1 2)(3 4)	15
(1 2 3)	20
(1 2 3 4 5)	12
(1 3 5 2 4)	12

(c) By Proposition 3.12 of Chapter 5, we know that any normal subgroup of A_5 is a union of conjugacy classes, so that any non-trivial normal subgroup must contain $\{e\}$ and at least one other conjugacy class. We also know that the order of a subgroup must divide $|A_5| = 60$.

Since it is impossible to find a union of conjugacy classes of A_5 that includes the identity and at least one other class that is not the whole group, and whose size divides 60, we conclude that A_5 has no proper non-trivial normal subgroups and is therefore a simple group.

Chapter 8

The Sylow Theorems

Introduction

Lagrange's Theorem tells us that in any finite group G the order of a subgroup H divides the order of G. However, the theorem says nothing about the *existence* of the subgroups of the possible orders: indeed, we know that G may fail to have a subgroup corresponding to some divisors of its order. For example, the alternating group A_4 of order 12 has no subgroup of order 6. However, we will show that there is a subgroup corresponding to every *prime power* divisor of the order of the group. This theorem will be the main result of this chapter. It ensures that, for example, a group of order

$$24 = 8 \times 3 = 2^3 \times 3$$

has subgroups of orders 2, 2^2, 2^3 and 3.

Any subgroup whose order is the highest power of a particular prime dividing the order of the group has additional properties that can be of assistance in classifying the groups of a given order. For example, the theorems that we prove will enable us to say that any group of order $91 = 7 \times 13$ must have a normal subgroup of order 13. This, in turn, will enable us to show that any group of order 91 is cyclic.

For a group of order 24, 2^3 is the highest power of 2 dividing the order.

Broadly speaking, the results that we will prove guarantee the existence of subgroups corresponding to prime power divisors of the order of a group and provide restrictions on the number of such subgroups a group can possess.

These results are due to the Norwegian mathematician L. Sylow (1832–1918). The original proofs start by considering the special case of abelian groups. However, the tools provided by group actions give more concise proofs, and these are the proofs we give.

The name Sylow is usually pronounced as 'Seeloff' or 'Seelow'.

The first section of this chapter introduces and proves these important results. In Subsection 1.1, we introduce a new group action and investigate its application to some particular examples. These examples will point the way to the general results that are needed. The use of group actions requires us to know the number of elements in the set being acted on. In the actions that we use, this involves knowledge of certain binomial coefficients.

Subsection 1.2 generalises the special cases of Subsection 1.1 to provide a proof of the first two of the Sylow Theorems.

Subsection 1.3 completes the proofs of Sylow's results with a proof of his third theorem.

In Section 2, we apply the results obtained to finite abelian groups and to other groups of various orders.

Section 3 shows that some of the results generalise to any prime power divisor of the order of a group.

The final section of this chapter and this book starts with a series of exercises that pulls together many of the ideas we have covered so far in

Book B in order to find all the possible groups of order $2p^2$, where p is an odd prime.

Chapter guide

Section 1 is a rather long one, with three subsections of roughly equal length in terms of study time. Section 2 consists mainly of exercises and thus will require a similar amount of study time in spite of being shorter. In compensation, Sections 3 and 4 are rather shorter.

The theorems proved in this chapter are powerful, general ones. It follows that some of the work, in Subsection 1.2 and Section 3 in particular, is fairly theoretical. The proofs in these sections are pivotal in the development of the theory of finite groups. In this chapter, we are also interested in using these theorems to determine the structure of particular groups, and the exercises in Section 2 have been designed with this aim in mind. The exercises in Section 4 require results from the whole of Book B, so they will be useful for revision.

1 The Sylow Theorems

The Sylow Theorems are a series of powerful results that give a wealth of information about the possible orders and number of subgroups of a finite group. In particular, Sylow's First Theorem provides a partial converse to Lagrange's Theorem.

1.1 Sylow p-subgroups

In Chapter 6 we proved Cauchy's Theorem (Theorem 3.16), which states that if a finite group G has order n and a prime number p divides n, then G has a subgroup of order p. The main aim of this chapter is to establish the Sylow Theorems, the first of which is an extension of Cauchy's Theorem.

Theorem 1.1 *Sylow's First Theorem*

Let G be a finite group of order n and let p be a prime dividing n, where p^α is the highest power of p dividing n. Then G has a subgroup of order p^α.

The proof of this theorem is postponed until Subsection 1.2.

The subgroup of order p^α in the statement of the theorem is called a **Sylow p-subgroup** of G, and the divisor p^α of n, which is the largest power of p that divides n, is referred to as the **maximal prime power divisor** corresponding to p.

For example, the theorem tells us that the permutation group S_4, which has order $4! = 24$, has subgroups of orders $2^3 = 8$ and 3.

From Theorem 4.3 of Chapter 7, we know that a p-group has subgroups corresponding to every divisor of its order. Taken together with Sylow's First Theorem, this means that a finite group has a subgroup corresponding to *every* prime power divisor of its order. As this result is sometimes useful, we state it as a corollary.

Corollary 1.2

Let G be a finite group of order n and let p be a prime dividing n. If p^k divides n then G has a subgroup of order p^k.

Hence the permutation group S_4 has subgroups of orders 2 and $2^2 = 4$ as well as the ones mentioned above.

In Example 1.3 we illustrate the structure of the proof of Sylow's First Theorem by considering a specific example, and we introduce the group action that we will use later to prove the theorem. The group action we want is a generalisation of the action of a group on itself by left multiplication.

Example 1.3 *Subgroups of a group of order 20*

Let G be any group of order $20 = 2^2 \times 5$. The order of G is divisible by the primes 2 and 5. The maximal prime power divisors of $|G|$ corresponding to 2 and 5 are $2^2 = 4$ and $5^1 = 5$, respectively.

We show that G must have a subgroup of order 4.

Let X be the collection of all four-element subsets of G. We define an action of the group G on the set X by

$$g \wedge A = gA = \{ga : a \in A\}$$

for every element A of X.

Note that this is different from our proof of Cauchy's Theorem, where the set acted upon consisted of tuples of elements rather than subsets. Since these are subsets, the four elements are distinct.

Thus, G acts on X by left multiplication.

In order to verify that we have indeed defined a group action according to Definition 3.1 of Chapter 6, we must show that $g \wedge A$ is an element of X for all $g \in G$ and $A \in X$, and that:

(a) $e \wedge A = A$ for all $A \in X$

(b) $(gh) \wedge A = g \wedge (h \wedge A)$ for all $g, h \in G$ and $A \in X$.

So that we do not break the flow of the example, we ask you to check that this is an action in a more general case in Exercise 1.2 below.

As for any group action, we can immediately make two statements. One comes from the fact that the orbits partition X; the other comes from the Orbit–Stabiliser Theorem, that is, Corollary 3.13 of Chapter 6.

Suppose that $\mathrm{Orb}(A_1), \mathrm{Orb}(A_2), \ldots, \mathrm{Orb}(A_s)$ are the distinct orbits for this group action. We know these orbits partition X, so

$$|X| = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|.$$

We call this the **partition equation**. By the Orbit–Stabiliser Theorem,

$$|G| = |\mathrm{Orb}(A_i)| \times |\mathrm{Stab}(A_i)|, \quad i = 1, \ldots, s.$$

Since we are searching for a subgroup of order 4, we could show that one of the four-element subsets that are the elements of X must be a subgroup of G. Alternatively, we could show that one of the stabilisers, which we know are subgroups of G, must have four elements. Both approaches are possible; we choose the second.

To make use of the equations above, we need to know $|X|$, the size of X. Since G has 20 elements, the number of four-element subsets of G is the number of ways of choosing four elements from 20, that is,

The **binomial coefficient** ${}^nC_r$ can be calculated from
$${}^nC_r = \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}.$$

$$\begin{aligned} {}^{20}C_4 &= \frac{20 \times 19 \times 18 \times 17}{4 \times 3 \times 2 \times 1} \\ &= \frac{5 \times 19 \times 9 \times 17}{1 \times 3 \times 1 \times 1} \\ &= 5 \times 19 \times 3 \times 17 \\ &= 4845. \end{aligned}$$

Hence $|X| = 4845$ and the partition equation is

$$4845 = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|.$$

The Orbit–Stabiliser Theorem gives

$$20 = |\mathrm{Orb}(A_i)| \times |\mathrm{Stab}(A_i)|, \quad i = 1, \ldots, s.$$

We will use these equations to deduce that there is a stabiliser whose order is 4. By the Orbit–Stabiliser Theorem, the orbit corresponding to such a stabiliser has size 5, which is not divisible by 2. This observation prompts us to look for an orbit whose size is not divisible by 2.

If all the terms in the sum on the right-hand side of the partition equation were divisible by 2, then so would be the left-hand side. But the left-hand side, 4845, is *not* divisible by 2, so we can deduce that at least one of the terms

$$|\mathrm{Orb}(A_1)|, |\mathrm{Orb}(A_2)|, \ldots, |\mathrm{Orb}(A_s)|$$

on the right-hand side is not divisible by 2. Therefore there is an element A of X such that

$$|\mathrm{Orb}(A)|$$

is not divisible by 2.

Applying the Orbit–Stabiliser Theorem to A gives

$$|G| = 20 = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

Since $|\mathrm{Orb}(A)|$ is not divisible by 2 and $|G|$ is divisible by 4, it follows that $|\mathrm{Stab}(A)|$ is divisible by 4. From this we deduce that

$$|\mathrm{Stab}(A)| \geq 4.$$

So far we have established the existence of a *subgroup* $\mathrm{Stab}(A)$ of G of order at least 4. If we could show that $|\mathrm{Stab}(A)| \leq 4$, the proof would be complete.

So far we have used the partition equation of the group action and the Orbit–Stabiliser Theorem, but not the fact that the elements of X are subsets of the group G. We will now exploit this fact as we inspect carefully the consequences of the definition of a stabiliser.

Suppose that g is any element of $\mathrm{Stab}(A)$. Then $g \wedge A = A$. Now choose a fixed element a in A. Since our action is defined by left multiplication, we have

$$ga \in g \wedge A = A.$$

So $ga \in A$ for every element g in $\mathrm{Stab}(A)$.

If we consider all the elements of the form ga, for g in $\mathrm{Stab}(A)$, we obtain the right coset

$$\mathrm{Stab}(A)a$$

of $\mathrm{Stab}(A)$. We have just shown that all elements of this right coset are in A. Hence

$$\mathrm{Stab}(A)a \subseteq A.$$

Thus, $\mathrm{Stab}(A)a$ cannot have more elements than A, and so

$$|\mathrm{Stab}(A)a| \leq |A| = 4.$$

However, right cosets have the same number of elements as the subgroup from which they are formed. Thus

$$|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq 4.$$

This provides the other inequality that we wanted and we deduce that

$$|\mathrm{Stab}(A)| = 4.$$

We have shown the existence of a subgroup $\mathrm{Stab}(A)$ of G that has order 4, as required.

Thus, we have shown that any group G of order 20 has a Sylow 2-subgroup of order 4.

Exercise 1.1

Adapt the argument used in Example 1.3 to show that any group of order 20 must have a Sylow 5-subgroup of order 5. You should define an appropriate group action, but you need not prove that it is an action.

To complete the arguments used in Example 1.3 and in the solution to Exercise 1.1, we need to prove that the group actions we defined are indeed actions. You are asked to do this in the next exercise.

Exercise 1.2

Let G be a finite group and let X be the set of all subsets of G that have exactly k elements. Define

$$g \wedge A = gA$$

for every $g \in G$ and $A \in X$.

Show that this defines an action of G on X by proving that $g \wedge A$ is an element of X, that is, it is a k-element subset, and that for all $g, h \in G$ and $A \in X$:

(a) $e \wedge A = A$

(b) $(gh) \wedge A = g \wedge (h \wedge A)$.

We now examine the key steps in Example 1.3 and in the solution to Exercise 1.1 to see what we need to do to generalise the proofs.

Suppose that G is a group of order n, that p is a prime that divides n, and that p^α is the highest power of p that divides n. In this setting, the key steps in Example 1.3 and Exercise 1.1 generalise as follows.

1. Define X to be the set consisting of all subsets of G containing p^α elements.
2. Define an action of G on X by left multiplication, that is,

   $$g \wedge A = gA, \quad g \in G,\ A \in X.$$

   The solution to Exercise 1.2 ensures that this *is* a group action.
3. Show that $|X|$ is not divisible by p.
4. Suppose that $\mathrm{Orb}(A_1), \mathrm{Orb}(A_2), \ldots, \mathrm{Orb}(A_s)$ are the distinct orbits for this group action and deduce from the partition equation

   $$|X| = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|$$

   that at least one orbit has order not divisible by p.
5. If A is an element in X such that $|\mathrm{Orb}(A)|$ is not divisible by p, use the Orbit–Stabiliser Theorem

   $$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|$$

   to deduce that $|\mathrm{Stab}(A)|$ is divisible by p^α. Hence

   $$|\mathrm{Stab}(A)| \geq p^\alpha.$$
6. Show that, for a fixed element a of A,

   $$\mathrm{Stab}(A)a \subseteq A$$

   and, hence, that

   $$|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq |A| = p^\alpha.$$

   Since both $\mathrm{Stab}(A)a$ and A have p^α elements and $\mathrm{Stab}(A)a \subseteq A$, we have $\mathrm{Stab}(A)a = A$.
7. Conclude that $\mathrm{Stab}(A)$ has p^α elements and so it is a subgroup of G of order p^α.

We can extract three results from the above proof strategy that it is useful to summarise in the following lemma. The proofs of parts (a) and (b) are given after the proof of Sylow's First Theorem, in Subsection 1.2. The proof of part (c) follows directly from the marginal note next to step 7 above.

Lemma 1.4

Let G be a finite group and let X be the set of all the k-element subsets of G. If G acts by left multiplication on X and if $A \in X$, then:

(a) $|\mathrm{Stab}(A)|$ divides $|A|$.

(b) If k is a power of a prime p, then $\mathrm{Stab}(A)$ is a p-group.

(c) If k is the maximal power of p dividing the order of G and if p does not divide $|\mathrm{Orb}(A)|$, then

$$\mathrm{Stab}(A)a = A \quad \text{for any } a \in A.$$

In Example 1.3 we could replace the order of the group, 20, with a general value n, and the prime 2 with a general prime p, throughout, and still have a valid proof except at one point. One crucial step involved observing that the number of elements of X was not divisible by 2. For a general proof we would have to show the corresponding statement that if p^α is the highest power of p dividing the order of the group, then the number of p^α-element subsets of the group is not divisible by p. That is, we would have to show that the binomial coefficient ${}^nC_{p^\alpha}$ is not divisible by p.

We will consider such divisibility properties of binomial coefficients in Subsection 1.2. Once we have shown that ${}^nC_{p^\alpha}$ is not divisible by p, the discussion above shows that all the other steps in the argument do generalise and so give a proof of Sylow's First Theorem.

Exercise 1.3

(a) Show that ${}^{24}C_3$ is not divisible by 3, and hence that any group of order 24 has a subgroup of order 3.

(b) Show that any group of order 24 has a subgroup of order 8.

(c) Let G be a group of order 15. Show that G has a subgroup H of order 3 and a subgroup K of order 5.

The solution to Exercise 1.3 is quite instructive, in that the details of the calculations in parts (a) and (b) give some indication of why the binomial coefficient ${}^{24}C_3$ is not divisible by 3 and why the binomial coefficient ${}^{24}C_8$ is not divisible by 2. In the first case, the only term in the numerator divisible by 3 is 24, and its factor of 3 cancels with the corresponding term 3 in the denominator. In the second case, every term in the original numerator divisible by a power of 2 has a corresponding term in the denominator divisible by the same power of 2. Also note that in the

solution to part (c), the cancellations occur in corresponding terms as in the previous solutions.

The second and third Sylow Theorems, which we discuss later in this chapter, are concerned with the number of different Sylow p-subgroups corresponding to the prime p. To conclude this subsection, we investigate an example that indicates the nature of these results and which leads to a formulation of Sylow's Second Theorem.

Example 1.5 *Sylow 5-subgroups in groups of order 15*

We continue the investigation of groups of order 15, using the same notation as in Exercise 1.3(c).

Let G be a group of order 15, let X be the set of all five-element subsets of G and let

$$\mathrm{Orb}(A_1), \ldots, \mathrm{Orb}(A_s)$$

be the distinct orbits under the action of G on X by left multiplication.

Since the Sylow 5-subgroups contain five elements, they are elements of X. Thus each 5-subgroup must be contained in some orbit of the action. We claim that the orbits that contain these subgroups are precisely the ones whose size is not divisible by 5, and that each such orbit contains exactly one Sylow 5-subgroup. Thus, counting the number of Sylow 5-subgroups is the same as counting the number of orbits whose size is not divisible by 5.

Our claim will be proved in the following three steps.

1. If $A \in X$ is such that 5 does not divide $|\mathrm{Orb}(A)|$, then $\mathrm{Orb}(A)$ contains a Sylow 5-subgroup.
2. If $\mathrm{Orb}(A)$ contains a Sylow 5-subgroup then 5 does not divide $|\mathrm{Orb}(A)|$.
3. Any orbit can contain at most one Sylow 5-subgroup.

Let us now go through each step.

1. If 5 does not divide $|\mathrm{Orb}(A)|$, we know from the proof strategy of Sylow's First Theorem that $\mathrm{Stab}(A)$ is a Sylow 5-subgroup. Call this subgroup H.

   Let $a \in A$. Then by Lemma 1.4 we have

   $$Ha = A.$$

   Now the orbit of A includes

   $$a^{-1} \wedge A = a^{-1}A = a^{-1}Ha.$$

   But $a^{-1}Ha$ is the conjugate of H by a^{-1}, and so it is a subgroup of G with the same order as H. This is because whenever H is a subgroup of a group G and $g \in G$, then gHg^{-1} is also a subgroup of G of the same order as H.

   Therefore $a^{-1}Ha$ is a Sylow 5-subgroup contained in $\mathrm{Orb}(A)$.

2. Suppose that $\mathrm{Orb}(A)$ contains the Sylow 5-subgroup H. This means that $\mathrm{Orb}(H) = \mathrm{Orb}(A)$.

   In order to show that $|\mathrm{Orb}(A)|$ is not divisible by 5, we show that $\mathrm{Stab}(H) = H$ and use the Orbit–Stabiliser Theorem.

   Let $g \in G$. Then

   $$g \wedge H = gH.$$

   Now $gH = H$ if, and only if, $g \in H$. That is, $g \in \mathrm{Stab}(H)$ if, and only if, $g \in H$. Thus $\mathrm{Stab}(H) = H$.

   The Orbit–Stabiliser Theorem gives

   $$|G| = 15 = |\mathrm{Orb}(H)| \times |\mathrm{Stab}(H)| = |\mathrm{Orb}(H)| \times 5.$$

   This shows that $|\mathrm{Orb}(H)|$, and hence $|\mathrm{Orb}(A)|$, is not divisible by 5.

3. Suppose $\mathrm{Orb}(A)$ contains the Sylow 5-subgroup H. Then, as before,

   $$\mathrm{Orb}(A) = \mathrm{Orb}(H) = \{gH : \ g \in G\}.$$

   Thus the orbit of A consists of all left cosets of H. Only one of these cosets is a subgroup, namely H itself, because only H contains the identity e.

We have shown that there is exactly one Sylow 5-subgroup in each of the orbits whose size is not divisible by 5, and no Sylow 5-subgroup in any orbit whose size is divisible by 5. Furthermore, all the Sylow 5-subgroups are accounted for in this way since, for any Sylow 5-subgroup H, we have $H \in X$ and $H \in \mathrm{Orb}(H)$.

We can now use the partition equation for the action to say more about the number of Sylow 5-subgroups.

Suppose that G has m distinct subgroups of order 5, which we call

$$H_1, \ldots, H_m.$$

Each of these belongs to a distinct orbit and so we can write the partition equation as

$$\begin{aligned} |X| &= 3003 \\ &= |\mathrm{Orb}(H_1)| + \cdots + |\mathrm{Orb}(H_m)| + |\mathrm{Orb}(A_{m+1})| + \cdots + |\mathrm{Orb}(A_s)|, \end{aligned}$$

where the sizes of the first m orbits are not divisible by 5 and the sizes of the remaining orbits are.

By the Orbit–Stabiliser Theorem,

$$|G| = 15 = |\mathrm{Orb}(H_i)| \times |\mathrm{Stab}(H_i)|, \quad i = 1, \ldots, m.$$

We showed above that

$$\mathrm{Stab}(H_i) = H_i, \quad i = 1, \ldots, m$$

and so

$$|\mathrm{Stab}(H_1)| = \cdots = |\mathrm{Stab}(H_m)| = 5.$$

Hence

$$|\mathrm{Orb}(H_1)| = \cdots = |\mathrm{Orb}(H_m)| = 3.$$

The sizes of the remaining orbits are divisible by 5, so we have

$$|X| = 3003 = 3m + (\text{a multiple of } 5).$$

Reducing this equation modulo 5 gives

$$3 \equiv 3m \pmod 5.$$

Multiplying both sides by 2, and observing that $2 \times 3 = 6$ is congruent to 1 modulo 5, gives

$$m \equiv 1 \pmod 5.$$

Thus, in any group of order 15, the number of Sylow 5-subgroups is congruent to 1 modulo 5.

In Subsection 1.2 we will show that the argument above generalises to give the following theorem.

Theorem 1.6 *Sylow's Second Theorem*

Let G be a finite group of order n and let p be a prime dividing n. Then the number of distinct Sylow p-subgroups of G is congruent to 1 modulo p.

We ask you to take Sylow's Second Theorem on trust for now. To give an example of its use, the next exercise asks you to apply it to classify all groups of order 15.

Exercise 1.4

Let G be a group of order 15.

(a) Show that two distinct Sylow 5-subgroups of G must have trivial intersection.

(b) Assume that G has m Sylow 5-subgroups and that Sylow's Second Theorem holds, that is, that m is congruent to 1 modulo 5. By counting elements of order 5, show that G has exactly one subgroup of order 5 and hence only four elements of order 5.

(c) Let l be the number of Sylow 3-subgroups of G. Determine, in terms of l, the number of elements of G of order 3.

(d) Assume that Sylow's Second Theorem holds, that is, that l is congruent to 1 modulo 3. By counting the number of elements of G of orders 1, 3 and 5, show (by contradiction) that G has an element of order 15 and, hence, that G is cyclic.

So Sylow's First and Second Theorems have enabled us to show that the only group of order 15 is $\mathbb{Z}_{15}$ (since, as we saw in Chapter 6, all cyclic groups of order n are isomorphic to $\mathbb{Z}_n$). You now know all about the groups of order up to and including 15.

1.2 Sylow's First and Second Theorems

Our main aim in this subsection is to give formal proofs of Sylow's First and Second Theorems. For reference, we restate the first theorem and the related definitions.

Definition 1.7 *Sylow p-subgroup*

Let G be a finite group of order n and let p be a prime dividing n. Let p^α be the highest power of p dividing n. Then a subgroup of G of order p^α is called a **Sylow p-subgroup** of G.

Sylow's First Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then G has a Sylow p-subgroup.

As we indicated in Subsection 1.1, our proof of Sylow's First Theorem will use the action of G defined by left multiplication on the set X of all p^α-element subsets of G.

In Subsection 1.1, we noted that a crucial step in the argument was to show that the size of X is not divisible by p. Since the size of X is given by the number of ways of choosing p^α elements from n elements, we have

$$|X| = {}^nC_{p^\alpha}.$$

We therefore need to consider which powers of p can divide this binomial coefficient.

Example 1.3 from Subsection 1.1 and the discussion following Exercise 1.3 give some clues as to how a general proof can be constructed. In Example 1.3 we had a group of order 20 and considered the set X of all four-element subsets of the group. The calculation of the binomial coefficient is, in detail,

$$\begin{aligned} |X| &= {}^{20}C_4 \\ &= \frac{20 \times (20-1) \times (20-2) \times (20-3)}{4 \times (4-1) \times (4-2) \times (4-3)} \\ &= \frac{5 \times (20-1) \times (10-1) \times (20-3)}{1 \times (4-1) \times (2-1) \times (4-3)}. \end{aligned}$$

The important observation for our current purposes is that any power of 2 that divides a term in the numerator also divides the corresponding term in the denominator, and conversely.

This example suggests that we should write the general formula for the binomial coefficient that we require in the form

$$
\begin{aligned}
{}^{n}C_{p^\alpha} &= \frac{n \times (n-1) \times \cdots \times (n-(p^\alpha-1))}{p^\alpha \times (p^\alpha-1) \times \cdots \times 1} \\
&= \frac{(n-0) \times (n-1) \times \cdots \times (n-(p^\alpha-1))}{(p^\alpha-0) \times (p^\alpha-1) \times \cdots \times (p^\alpha-(p^\alpha-1))}.
\end{aligned}
$$

Given the conditions of Sylow's First Theorem, we can write

$$n = p^\alpha z,$$

where z is not divisible by p. The expression for the binomial coefficient becomes

$${}^{p^\alpha z}C_{p^\alpha} = \frac{(p^\alpha z-0) \times (p^\alpha z-1) \times \cdots \times (p^\alpha z-(p^\alpha-1))}{(p^\alpha-0) \times (p^\alpha-1) \times \cdots \times (p^\alpha-(p^\alpha-1))}.$$

Each term in the numerator is of the form

$$p^\alpha z - k,$$

where $k = 0, \ldots, p^\alpha - 1$. The corresponding terms in the denominator are of the form

$$p^\alpha - k,$$

where $k = 0, \ldots, p^\alpha - 1$.

The case of ${}^{20}C_4$ considered above suggests that the highest powers of p dividing $p^\alpha z - k$ and $p^\alpha - k$ are the same, for each value of k from 0 to $p^\alpha - 1$ (and are in fact the highest power of p dividing k). You will establish this result in the next exercise, which uses the notation described above.

Exercise 1.5

(a) Let k be an integer such that $0 < k < p^\alpha$.

(i) Show that if p^β divides $p^\alpha z - k$, then $\beta < \alpha$.

(ii) Hence show that p^β divides $p^\alpha z - k$ if, and only if, p^β divides k.

(b) Deduce that if p does not divide z, then

$${}^{p^\alpha z}C_{p^\alpha}$$

is not divisible by p.

As we indicated in Subsection 1.1, the fact that if p is a prime that does not divide z then ${}^{p^\alpha z}C_{p^\alpha}$ is not divisible by p is the key to providing a general proof of Sylow's First Theorem.

The special cases dealt with in Subsection 1.1 can now be translated directly into a general proof.

Proof of Sylow's First Theorem Let X be the set of all subsets of G having p^α elements, and let G act on X by left multiplication. Suppose that the distinct orbits under this action are

You have shown in Exercise 1.2 that this *is* a group action.

$$\mathrm{Orb}(A_1), \ldots, \mathrm{Orb}(A_s).$$

By the partition equation we know that

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|.$$

The use of group actions to prove Sylow's First Theorem is due to H. Wielandt (in 1959), although the result itself has been established for over a century.

By Exercise 1.5, the left-hand side is not divisible by p. Hence at least one term on the right-hand side is not divisible by p.

Let A be an element of X such that $|\mathrm{Orb}(A)|$ is not divisible by p. The Orbit–Stabiliser Theorem gives

$$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

But $|G|$ is divisible by p^α and $|\mathrm{Orb}(A)|$ is not divisible by p. It follows that $|\mathrm{Stab}(A)|$ is divisible by p^α. Thus $|\mathrm{Stab}(A)| \geq p^\alpha$.

Now consider any element g of $\mathrm{Stab}(A)$ and fix an element a of A. Since $\mathrm{Stab}(A)$ is the stabiliser of A,

$$ga \in g \wedge A = A.$$

Thus, $ga \in A$ for every element $g \in \mathrm{Stab}(A)$. This implies that

This particular part of the proof does *not* use the fact that $|\mathrm{Orb}(A)|$ is not divisible by p.

$$\mathrm{Stab}(A)a \subseteq A.$$

Hence $|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq |A| = p^\alpha$.

It follows that $|\mathrm{Stab}(A)| = p^\alpha$. Thus $\mathrm{Stab}(A)$ is a subgroup of G with order p^α, completing the proof. ■

The action of G on the set X of p^α-element subsets of G provides rather more information than is actually used in the proof of Sylow's First Theorem.

In the proof, the existence of a Sylow p-subgroup was established by showing that the stabiliser of some element $A \in X$ had the correct order. The proof shows that the stabiliser of any $A \in X$, such that $|\mathrm{Orb}(A)|$ is not divisible by p, is a Sylow p-subgroup of G. We will show later that all Sylow p-subgroups arise in this way.

Some parts of the proof did not depend on $|\mathrm{Orb}(A)|$ not being divisible by p. In particular, if $a \in A$ and $g \in \mathrm{Stab}(A)$ then

$$ga \in g \wedge A = A,$$

and so all the elements of the right coset $\mathrm{Stab}(A)a$ are contained in A. On the other hand, if a is any element of A, then a is in the right coset $\mathrm{Stab}(A)a$. Thus any $A \in X$ is the union of some right cosets of its stabiliser $\mathrm{Stab}(A)$, those given by elements of A. Since distinct right cosets are disjoint, this means that A consists of a union of disjoint right cosets of $\mathrm{Stab}(A)$. Because all right cosets have the same size as $\mathrm{Stab}(A)$, $|\mathrm{Stab}(A)|$

divides $|A|$ for any A in X. This argument formalises the proof of Lemma 1.4(a).

Now, as A has p^α elements, the group $\mathrm{Stab}(A)$ is a p-group for any element $A \in X$, whether or not $\mathrm{Stab}(A)$ is a Sylow p-subgroup. This formalises the proof of Lemma 1.4(b).

Let us now move on towards proving Sylow's Second Theorem. We begin with a preliminary result.

Lemma 1.8

Let G be a finite group of order $p^\alpha z$, where p is a prime not dividing z. Let X be the set of p^α-element subsets of G. Then, in the action of G on X by left multiplication, the size of every orbit is divisible by z.

Proof Let G act on X by left multiplication. Then, for any $A \in X$, the Orbit–Stabiliser Theorem gives

$$|G| = p^\alpha z = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

By Lemma 1.4(b), we know that $\mathrm{Stab}(A)$ is a p-group. It follows that $|\mathrm{Orb}(A)|$ is divisible by z. ■

This lemma gives useful information about the number of Sylow p-subgroups, and it is used in the proof of Sylow's Second Theorem.

In Example 1.5, we saw that in a group of order 15 the number of Sylow 5-subgroups is congruent to 1 modulo 5. This result generalises to give Sylow's Second Theorem, which we restate and prove.

Sylow's Second Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then the number of distinct Sylow p-subgroups of G is congruent to 1 modulo p.

Proof Our proof uses the same group action and notation as the proof of Sylow's First Theorem.

This strategy generalises a result we obtained in Example 1.5 of Subsection 1.1.

The strategy for the proof is to show that Sylow p-subgroups are exactly the stabilisers of elements whose orbits have size not divisible by p and that each such orbit contains exactly one Sylow p-subgroup. We then use the partition equation

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|$$

to obtain the required result.

We start by showing that if $A \in X$ is such that $|\mathrm{Orb}(A)|$ is not divisible by p, then $\mathrm{Orb}(A)$ contains a Sylow p-subgroup. Under these conditions we know, from our proof of Sylow's First Theorem, that $H = \mathrm{Stab}(A)$ is a Sylow p-subgroup. We also know, by Lemma 1.4, that for a fixed element $a \in A$, $Ha = A$.

Now the orbit of A includes $a^{-1} \wedge A = a^{-1}A = a^{-1}Ha$. But $a^{-1}Ha$ is the conjugate of H by a^{-1}, and so it is a subgroup of G with the same order as H. In other words, $a^{-1}Ha$ is a Sylow p-subgroup contained in $\mathrm{Orb}(A)$. Thus every orbit whose size is not divisible by p contains a Sylow p-subgroup as an element.

Conversely, consider a Sylow p-subgroup H of G. By the definition of X, the subgroup H is an element of X because $|H| = p^\alpha$. We will show that the stabiliser of H is H itself, that is $\mathrm{Stab}(H) = H$, and hence that H is in an orbit, $\mathrm{Orb}(H)$, whose size is not divisible by p.

By the definition of the action, if $g \in G$ then $g \wedge H = gH$, a left coset of H in G. However, we know that $gH = H$ if, and only if, $g \in H$. So $g \wedge H = H$, i.e. $g \in \mathrm{Stab}(H)$ if, and only if, $g \in H$. This shows that $\mathrm{Stab}(H) = H$. The Orbit–Stabiliser Theorem gives

$$\begin{aligned} p^\alpha z &= |G| \\ &= |\mathrm{Orb}(H)| \times |\mathrm{Stab}(H)| \\ &= |\mathrm{Orb}(H)| \times |H| \\ &= |\mathrm{Orb}(H)| \times p^\alpha. \end{aligned}$$

Hence $|\mathrm{Orb}(H)| = z$ and is not divisible by p, and of course $H \in \mathrm{Orb}(H)$.

We now know that an orbit contains a Sylow p-subgroup if, and only if, the size of the orbit is not divisible by p. The last main step is to show that an orbit can contain at most one Sylow p-subgroup.

Let H be a Sylow p-subgroup. Then $\mathrm{Orb}(H)$ consists of all $g \wedge H = gH$ for $g \in G$, that is, all left cosets of H. However, the only left coset of the subgroup H that is a subgroup of G is H itself. Hence no orbit can contain more than one Sylow p-subgroup.

Thus we have established that each orbit whose size is not divisible by p contains exactly one Sylow p-subgroup and that the orbits whose size is divisible by p contain no Sylow p-subgroups. Hence the number of Sylow p-subgroups is the number of orbits whose size is not divisible by p.

We now separate the terms on the right-hand side of the partition equation

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|$$

into those that are divisible by p and those that are not.

Suppose that G has m distinct Sylow p-subgroups, so the action has m distinct orbits whose size is not divisible by p. We write the partition equation as

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_m)| + |\mathrm{Orb}(A_{m+1})| + \cdots + |\mathrm{Orb}(A_s)|,$$

where the first m terms on the right are not divisible by p and the remaining terms are.

For each of the first m terms, $\mathrm{Stab}(A_i)$ is a Sylow p-subgroup and the Orbit–Stabiliser Theorem gives

$$|G| = p^\alpha z = |\mathrm{Orb}(A_i)| \times |\mathrm{Stab}(A_i)| = |\mathrm{Orb}(A_i)| \times p^\alpha, \quad i = 1, \ldots, m.$$

Thus

$$|\mathrm{Orb}(A_i)| = z, \quad i = 1, \ldots, m.$$

By Lemma 1.8, *all* the terms in the partition equation are divisible by z. As we have seen, the first m terms are z. The remaining terms are divisible both by z and by p and, because p and z are coprime, are divisible by pz. Hence

$$|X| = mz + (\text{terms divisible by } pz),$$

which we can write as $|X| = mz + kpz$ for some integer k.

Before continuing, let us paraphrase the result that we have just obtained. Let G be any group of order $n = p^\alpha z$, where p is a prime that does not divide z. Let m be the number of Sylow p-subgroups of G. Then there exists an integer k (which depends on the specific group G) such that

$$|X| = {}^nC_{p^\alpha} = mz + kpz.$$

We now apply this result to the special case of the cyclic group $\mathbb{Z}_n$ of order n. In this case we know that there is exactly one subgroup belonging to each divisor of n. In particular, there is exactly one subgroup of order p^α, and so $m = 1$ for $\mathbb{Z}_n$. Hence, there exists an integer k' such that ${}^nC_{p^\alpha} = z + k'pz$. We now have two expressions for the binomial coefficient, which we equate:

$$mz + kpz = z + k'pz.$$

Dividing through by z gives $m + kp = 1 + k'p$. Hence, $m - 1 = k'p - kp = p(k' - k)$. So p divides $m - 1$ and $m \equiv 1 \pmod{p}$. This completes the proof. ■

Sylow's Second Theorem places sufficient restriction on the number of distinct Sylow p-subgroups for us to be able to make deductions about groups of some specific orders.

Exercise 1.6

Let G be a group of order 91.

(a) Show that G has only one Sylow 13-subgroup.

(b) By investigating the number of elements of order 7, show that G is cyclic.

Hint: in part (b), argue by contradiction.

We have discussed two examples of groups of order pq, where p and q are distinct primes, namely 15 and 91. On the basis of these examples, it would be tempting to believe that all such groups are cyclic. The existence of the dihedral group D_3 of order $6 = 2 \times 3$ is enough to dispel this belief. However, it is possible to make, and prove, a modified version of this conjecture. The next exercise provides a first step in this direction.

Exercise 1.7

(a) Let G be a group of order pq, where p and q are primes with $p < q$. Show that G has exactly one Sylow q-subgroup.

(b) By considering the order of the conjugates of the Sylow q-subgroup of G, show that it is normal in G.

Exercise 1.7 provides a complete generalisation of part of what we discovered about our earlier examples. For groups of this type, the Sylow q-subgroup (the one of larger prime order) is unique and hence normal.

It is worth observing that the proof of the normality of the Sylow q-subgroup in Exercise 1.7 did not use the fact that we were dealing with a Sylow subgroup, but only that there was a unique subgroup of that order. The solution therefore contains a proof of the following lemma.

Lemma 1.9

If G is a group that has only one subgroup of a particular order, then this subgroup is normal.

So far we have established two of the three results that are collectively known as the Sylow Theorems. The final result also concerns the number of Sylow p-subgroups. We have already shown that this number is congruent to 1 modulo p. It must also be a divisor of the order of the group, although establishing this requires a different group action from the proofs above. We deal with this matter in Subsection 1.3.

Finally, as we observed in Corollary 1.2, the Sylow p-subgroups are p-groups and therefore they contain subgroups corresponding to each divisor of their order. Thus, if G has a Sylow p-subgroup of order p^α, then G also has subgroups of orders

$$p, p^2, \ldots, p^{\alpha-1}.$$

We will consider the number of such subgroups, and provide an alternative proof of their existence, in Section 3.

1.3 Sylow's Third Theorem

In the process of classifying groups of a particular order, knowledge of subgroups is sometimes helpful. The Sylow Theorems provide information about subgroups, based only on the order of the group. In particular, as we have seen in some examples, for certain orders the groups must possess a *normal* Sylow p-subgroup. This knowledge can be useful in reducing the number of possibilities to be considered.

We have established two results about a group G of order $n = p^\alpha z$, where p does not divide z. Firstly, G has at least one subgroup of order p^α. Secondly, the number m of such subgroups is congruent to 1 modulo p.

In this subsection we establish that m divides the order of G. This restriction on m is often useful.

In fact, we establish rather more. Since the conjugate of any subgroup is a subgroup of the same order, we already know that the conjugate of a Sylow p-subgroup is another Sylow p-subgroup. We will prove the converse, that is, that any two Sylow p-subgroups are conjugate.

We will use one group action to establish that Sylow p-subgroups are conjugate and another, based on conjugacy, to derive the result that m divides $|G|$.

Exercise 1.8

Let G be a finite group whose order is divisible by p and let H, K be Sylow p-subgroups of G. Let X be the set of left cosets of K, and for $h \in H$ and $gK \in X$ define

$$h \wedge (gK) = (hg)K.$$

Show that this is an action of H on X.

Exercise 1.9

Let G be a finite group of order $p^\alpha z$, where z is not divisible by p. Let H, K be Sylow p-subgroups of G and X be the set of left cosets of K. Consider the group action of H on X described in Exercise 1.8.

(a) What is the order of X?

(b) Use the Orbit–Stabiliser Theorem to show that $|\mathrm{Orb}(gK)| = p^\beta$ for $0 \leq \beta \leq \alpha$, for every $g \in H$.

(c) Use the partition equation to show that there is some $a \in G$ with $|\mathrm{Orb}(aK)| = 1$.

(d) Show that H and K are conjugate.

The next exercise introduces a second group action and asks you to use it to prove a further result on the number of Sylow p-subgroups.

Exercise 1.10

Let G be a finite group of order $p^\alpha z$, where z is not divisible by p. Let

$$H_1, H_2, \ldots, H_m$$

be all the Sylow p-subgroups of G. Let $X = \{H_1, H_2, \ldots, H_m\}$, and for $g \in G$ and $H_i \in X$ define

$$g \wedge H_i = gH_ig^{-1}.$$

(a) Show that $\wedge$ defines an action of G on X.

(b) How many orbits does this action have?

(c) Use the Orbit–Stabiliser Theorem to show that m divides $|G|$.

Hint: for part (b), use Exercise 1.9.

The solutions to Exercises 1.9 and 1.10 provide the proof of Sylow's Third Theorem.

Theorem 1.10 *Sylow's Third Theorem*

Let G be a finite group. Then all the Sylow p-subgroups of G are conjugate, and the number of Sylow p-subgroups divides $|G|$.

There is a corollary to Sylow's Second and Third Theorems that is slightly easier to use for large values of $|G|$.

Corollary 1.11

Let G be a finite group of order $p^\alpha z$, where p is a prime not dividing z. Let m be the number of Sylow p-subgroups of G. Then m divides z.

Proof By Sylow's Second Theorem, we know that m is congruent to 1 modulo p, so p^α and m are coprime. By Sylow's Third Theorem, we know that m divides $|G| = p^\alpha z$. It follows that m divides z. ■

For reference, we present a complete statement of the Sylow Theorems.

Theorem 1.12 *The Sylow Theorems*

Let G be a finite group of order $n = p^\alpha z$, where p is a prime not dividing z. Let m be the number of subgroups of G of order p^α. Then:

- G has a Sylow p-subgroup, that is, $m \geq 1$
- $m \equiv 1 \pmod{p}$, that is, m is of the form $1 + kp$ for some integer k
- all the Sylow p-subgroups of G are conjugate
- m divides $|G|$, that is, m divides z.

The fact that the number of Sylow p-subgroups divides the order of the group provides shorter proofs of some of the results that have already been obtained.

Exercise 1.11

Let G be a group of order 15. Suppose that G has l Sylow 3-subgroups and m Sylow 5-subgroups.

(a) Show that $l = 1$.

(b) Show that $m = 1$.

(c) Show that G is cyclic.

Exercise 1.12

Let G be a group of order 6. Show that G has a unique Sylow 3-subgroup but could have either one or three Sylow 2-subgroups. By considering the groups of order 6, show that both possibilities occur.

2 Applications of the Sylow Theorems

Having proved the Sylow Theorems, we now investigate some applications.

2.1 Finite abelian groups

In Chapter 6 we were able to show that certain finite abelian groups are a direct product of cyclic groups. These are abelian groups whose order is a product of distinct primes and finite abelian p-groups (see Theorems 3.17 and 3.19 respectively). We are now in a position to extend these results to all finite abelian groups.

We start by proving a lemma based on Proposition 1.9 of Chapter 6.

Lemma 2.1

Let G be a finite abelian group with subgroups $H_1, H_2, \ldots, H_s$ such that $s \geq 2$ and

$$H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_s = \{e\}$$

for each i with $1 \leq i \leq s$.

Then $H_1 \times H_2 \times \cdots \times H_s$ is isomorphic to a subgroup of G.

Proof We prove this result by induction on s. When $s = 2$ the result follows directly from Proposition 1.9 of Chapter 6.

Suppose that the result is true for $s = k$; namely, suppose that if G has subgroups $H_1, H_2, \ldots, H_k$ such that

$$H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k = \{e\}$$

for each $i \in \{1, \ldots, k\}$, then $H_1 \times H_2 \times \cdots \times H_k$ is isomorphic to a subgroup of G.

Now suppose that G has subgroups $H_1, H_2, \ldots, H_{k+1}$ such that

$$H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{k+1} = \{e\}$$

for each $i \in \{1, \ldots, k+1\}$. Then for each $i \in \{1, \ldots, k\}$,

$$\{e\} = H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{k+1} \supseteq H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k,$$

since $e \in H_{k+1}$. Hence $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k = \{e\}$. Thus we can apply the induction hypothesis to deduce that $H = H_1 \times H_2 \times \cdots \times H_k$ is isomorphic to a subgroup of G.

Since G is abelian and $H_{k+1} \cap H = \{e\}$, we can now apply Proposition 1.9 of Chapter 6 to deduce that $H \times H_{k+1}$ is isomorphic to a subgroup of G.

The required result follows by (repeated applications of) Proposition 1.10 of Chapter 6 and mathematical induction. ■

Theorem 2.2

Let G be a finite abelian group of order $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes. Then

$$G \cong G_1 \times G_2 \times \cdots \times G_s,$$

where each G_i is an abelian group of order $p_i^{a_i}$ and hence a direct product of cyclic groups.

Proof By Theorem 1.1 (Sylow's First Theorem), we know that for each distinct prime p_i that divides n there is a Sylow p_i-subgroup G_i of order $p_i^{a_i}$.

Now for each i with $1 \leq i \leq s$,

$$G_i \cap G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_s = \{e\},$$

since the order of an element in G_i is coprime to the order of any element in $G_1G_2\cdots G_{i-1}G_{i+1}\cdots G_s$.

Thus, since G is abelian, Lemma 2.1 shows that $G_1 \times \cdots \times G_s$ is isomorphic to a subgroup of G. Since $|G|$ is the product of the orders of the Sylow p_i-subgroups, we can conclude that

$$G \cong G_1 \times \cdots \times G_s.$$

By Theorem 3.19 of Chapter 6, each G_i is a direct product of cyclic groups. The result then follows by Proposition 1.10 of Chapter 6. ■

We have now shown that every finite abelian group is (isomorphic to) a direct product of abelian groups of prime power order and hence can be factorised as a direct product of cyclic groups of prime power order. This decomposition into cyclic groups of prime power order is unique up to the order of the factors.

Exercise 2.1

Find the number of non-isomorphic abelian groups of order 72.

2.2 Exercises using the Sylow Theorems

This subsection consists mainly of exercises of three basic types.

Firstly, you are asked to find the number and type of Sylow subgroups of some specific groups. This process is sometimes referred to as 'finding the Sylow structure of a group'. Secondly, you are asked to use the Sylow Theorems to classify groups of a particular order. Thirdly, you are asked to use the Sylow Theorems to show that certain groups are simple; that is, that they contain no non-trivial, proper, normal subgroups.

This third type of activity needs some comment. When investigating the structure of a group G, the knowledge that G has a non-trivial, proper, normal subgroup N can be useful. We can look at the subgroup N and the quotient group G/N and use them to start building a composition series for G as in Subsection 4.2 of Chapter 7. If a group has a unique Sylow p-subgroup for some prime p, then by Lemma 1.9 the subgroup is normal and so, provided the group is not a p-group, the group cannot be simple.

In a p-group G, the unique Sylow p-subgroup is the whole of G, and so is not a proper subgroup.

We begin with the first type of activity by considering the Sylow subgroups of some familiar groups.

Exercise 2.2

For each of the following groups, find the Sylow p-subgroups for each prime dividing the order.

(a) $\mathbb{Z}_6$

(b) $\mathbb{Z}_3 \times \mathbb{Z}_{15}$

(c) S_3

We next look at the Sylow subgroups of some dihedral groups. When thinking about such groups, it is often useful to have in mind both their algebraic and geometric forms.

For example, geometrically D_7 is the group of symmetries of a regular heptagon (7-gon). Its elements are seven rotations about the centre through angles of $0, \frac{2\pi}{7}, \ldots, \frac{12\pi}{7}$ and seven reflections in the axes of symmetry. If we denote the rotation through $\frac{2\pi}{7}$ by a and a selected reflection by b, we obtain the presentation

$$D_7 = \langle a, b \mid a^7 = e,\ b^2 = e,\ ba = a^6 b\,(= a^{-1}b)\rangle.$$

When we do calculations within a dihedral group, sometimes it is easier to work with the presentation, sometimes with the geometry.

In Section 5 of Chapter 5 we mentioned the distinction between the direct and indirect symmetries of a plane figure. This distinction is relevant to our understanding of conjugacy in dihedral groups. Intuitively, for the symmetries of D_7 imagine that the heptagon is red on one side and blue on the other. Rotations preserve colour, reflections (carried out by turning the heptagon over) change the colour.

This observation makes it clear that conjugates of rotations are rotations. For if r is a rotation and g is any element of the group, consider grg^{-1}. Whatever g does to the colour, that is, preserves or changes it, g^{-1} does the same. Thus grg^{-1} must preserve colour and it is, therefore, a rotation.

Exercise 2.3

Consider the dihedral group D_7.

(a) Show that D_7 has a unique Sylow 7-subgroup.

(b) Using the fact that D_7 is not abelian, show that D_7 has exactly seven Sylow 2-subgroups.

(c) Deduce that all reflections are conjugate in D_7.

(d) Working from the presentation described above, show that each non-identity rotation is conjugate to itself and its inverse only.

(e) Write down the class equation for D_7 and hence find the centre of the group.

The class equation for a group appears in Theorem 2.6 of Chapter 7.

The next exercise asks you to use the Sylow Theorems to investigate groups of order 14. This gives an alternative approach to the one taken in Chapter 7.

Exercise 2.4

Show that there are only two groups of order 14, the cyclic group $\mathbb{Z}_{14}$ and the dihedral group D_7.

Hint: use the Sylow Theorems to deduce the existence of an element a of order 7 and an element b of order 2. By considering cosets, show that these two elements generate the group. By considering the conjugate of a by b, deduce the possible relations between a and b.

Many, but not all, of the results that were obtained in the solution to Exercise 2.3 apply to other dihedral groups.

Exercise 2.5

Consider the dihedral group D_{14} of order 28 with presentation

$$D_{14} = \langle a, b |\ a^{14} = e,\ b^2 = e,\ ba = a^{13}b\ (= a^{-1}b)\rangle.$$

(a) Show that D_{14} has a unique Sylow 7-subgroup.

(b) Show that the elements of D_{14} are of orders 1, 2, 7 and 14 only. Show also that there is exactly one rotation of order 2.

(c) Show that the product of two reflections is a rotation. Deduce that each Sylow 2-subgroup contains two distinct reflections and the unique rotation of order 2 (as well as the identity).

(d) Show that the subgroup $\{e, a^7\}$ is normal and that it is contained in every Sylow 2-subgroup of D_{14}.

(e) Show that D_{14} has exactly seven Sylow 2-subgroups.

In Exercise 1.3(c) we worked with a group of order 15. This is an example of a group of order pq, where p and q are distinct primes, that has a unique (normal) Sylow p-subgroup and a unique (normal) Sylow q-subgroup, from which facts we were able to deduce that the group is cyclic.

However, from our point of view, it is not the fact that the group is cyclic that is of particular interest, but rather that the group is, in fact, the internal direct product of its unique Sylow subgroups. To show that this is true in general, we need a special case of the Internal Direct Product Theorem (Theorem 1.5 of Chapter 6), which we restate here as a reminder.

Internal Direct Product Theorem

If H_1 and H_2 are subgroups of a group G, then

$$\phi : H_1 \times H_2 \to G$$
$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

When these three conditions are satisfied, we say that G is the **internal direct product** of H_1 and H_2.

In the case of a *finite* group, we have the following special case.

Theorem 2.3 *Internal direct product for finite groups*

If H_1 and H_2 are subgroups of a finite group G, then

$$\phi : H_1 \times H_2 \to G$$
$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism if all three of the following conditions hold:

(a) $|G| = |H_1| \times |H_2|$

(b) $|H_1|$ and $|H_2|$ are coprime

(c) H_1 and H_2 are normal subgroups of G.

Proof We are given that condition (c) of the Internal Direct Product Theorem holds, so we only need to show that $H_1 \cap H_2 = \{e\}$ and that $G = H_1 H_2$.

We know that $H_1 \cap H_2$ is a subgroup of both H_1 and H_2 by Proposition 2.6 of Chapter 5. Then $|H_1 \cap H_2|$ divides both $|H_1|$ and $|H_2|$ by Lagrange's Theorem. Since $|H_1|$ and $|H_2|$ are coprime,

$$|H_1 \cap H_2| = 1$$

and so the intersection is trivial, that is, $H_1 \cap H_2 = \{e\}$.

We can now apply Proposition 1.9 of Chapter 6 to conclude that $|H_1 H_2| = |H_1| \times |H_2|$. By condition (a), this implies that $|G| = |H_1 H_2|$, and hence that $G = H_1 H_2$.

All the conditions of the Internal Direct Product Theorem are satisfied and so $G \cong H_1 \times H_2$, as required. ■

We make two observations about this theorem and proof.

Firstly, the proof can be extended to cover more than two normal subgroups with orders coprime in pairs, the product of whose orders is the order of the group. Formally, this extension requires the Principle of Mathematical Induction. Care is needed when checking the second condition of Corollary 1.7 of Chapter 6.

Secondly, we will often apply Theorem 2.3 when the subgroups are unique Sylow subgroups for various primes. In this case the coprimeness of the orders is guaranteed, as is the product property, and normality is a consequence of the uniqueness.

The group of order 15 that we have already looked at in various ways is of this type. We know that it has a unique Sylow 3-subgroup and a unique Sylow 5-subgroup, both of which are cyclic and which have coprime orders. The group is, therefore, the internal direct product of these subgroups. The cyclicity of the group follows from what we know about the direct product of cyclic groups of coprime orders.

Exercise 2.6

(a) Let G be a group of order 221. Show that G is cyclic.

(b) Why does the argument used in the case $|G| = 221$ fail for a group of order 111?

Finally, you are asked to show that groups of particular orders cannot be simple.

Exercise 2.7

Let G be a group of order 110. Show that G has a non-trivial, proper, normal subgroup.

Exercise 2.8

Show that a group of order 132 cannot be simple.

Hint: consider the possibility that none of the Sylow subgroups is unique and show that this leads to a contradiction.

3 Subgroups of prime power order

The Sylow Theorems deal with the existence and number of Sylow p-subgroups for any prime p dividing the order of the group. Thus if G is a group with

$$|G| = p^\alpha z,$$

where p is prime and z is not divisible by p, then the theorems only give information about the subgroups of order p^α, and not about those of order p^β where $\beta < \alpha$.

As we observed earlier, in Subsection 1.1, because any Sylow p-subgroup H of a group G is a p-group, Theorem 4.3 of Chapter 7 shows that H has subgroups of each power of p from p^0 to p^α. This argument shows that G has subgroups corresponding to every power of p dividing $|G|$.

What is not obvious from this argument is that not only is the number of Sylow p-subgroups congruent to 1 modulo p, but the number of subgroups belonging to a particular integer power p^β of p, where $0 \leq \beta \leq \alpha$, is also congruent to 1 modulo p.

The proofs used for the first two of the Sylow Theorems can be adapted to deal with powers less than the highest. Such adaptation will give a second proof of the existence of such subgroups and also prove the 'congruent to 1 modulo p' result.

What cannot be generalised, because it is not true in general, is the conjugacy property of Sylow p-subgroups. Indeed, a group may have subgroups of the same prime power order that are not even isomorphic, so certainly cannot be conjugate. This is because conjugate subgroups are always isomorphic: by Proposition 2.1 of Chapter 7,

$$x \mapsto gxg^{-1}, \quad g, x \in G$$

defines an isomorphism from G to G that maps a subgroup H to its conjugate subgroup gHg^{-1}.

The next exercise provides an example of a group with non-isomorphic p-subgroups of the same order.

Exercise 3.1

Let D_4 be the dihedral group of order 8 with presentation

$$D_4 = \langle a, b \mid a^4 = e,\ b^2 = e,\ ba = a^{-1}b\ (= a^3b)\rangle.$$

(a) Show that D_4 has a cyclic subgroup of order 4.

(b) Show that $\{e, a^2, b, a^2b\}$ is a subgroup of order 4 isomorphic to the Klein group.

The solution to the previous exercise shows that D_4 has two non-isomorphic 2-subgroups of order 4. Thus the subgroups of D_4 with order 4 cannot all be conjugate.

Along with conjugacy, we also have to discard the result that the number of subgroups belonging to a particular prime power is a divisor of the order of the group. As our proof of the divisibility property used conjugacy, it is not entirely surprising that divisibility is lost too. You might wish to verify that D_4 has three subgroups of order 4, one cyclic and two isomorphic to the Klein group, and of course 3 does not divide $8 = |D_4|$.

Our aim, then, is to prove the following theorem.

Theorem 3.1 *Prime Power Subgroups Theorem*

Let G be a finite group and p be a prime.

If p^β divides $|G|$ then G has a subgroup of order p^β.

If m is the number of distinct subgroups of G of order p^β, then

$$m \equiv 1 \pmod{p}.$$

Our strategy for proving Theorem 3.1 is to examine the steps of the proofs of the first two Sylow Theorems and to generalise them.

The core of the original proofs was a group action on the set of p^α-element subsets of the group. For the generalisation, we define the set X on which G acts by left multiplication to be the set of all p^β-element subsets of G.

As in the first two Sylow Theorems, our proof will start by considering the size of X. We have

$$|X| = {}^nC_{p^\beta}.$$

Unlike in the proofs of the first two Sylow Theorems, this binomial coefficient may well be divisible by p, as the next exercise illustrates.

Exercise 3.2

Let G be a group of order 24 and let X be the set of four-element subsets of G.

(a) Calculate $|X|$.

(b) What is the highest power of 2 that divides $|X|$?

Let Y be the set of two-element subsets of G.

(c) Calculate $|Y|$.

(d) What is the highest power of 2 that divides $|Y|$?

Exercise 3.2 gives a hint as to the general result. For the 2^2-element subsets, 2^1 was the highest power dividing $|X|$. For the 2^1-element subsets, the highest power dividing $|Y|$ was 2^2. In each case, the combination of the size of the subsets and the size of the collection of subsets gave us 2^3 altogether, accounting for all the factors of 2 in the order of G.

Thus, if we are considering the set X of p^β-element subsets, we might expect the highest power of p that divides

$$|X| = {}^nC_{p^\beta}$$

to be $p^{\alpha-\beta}$. Once we establish this fact, the rest of the proof of Theorem 3.1 will follow those of the first two Sylow Theorems exactly.

Proof of Theorem 3.1 Suppose that $|G| = p^\alpha z$, where p does not divide z, and let $0 \leq \beta \leq \alpha$.

Let X be the set of p^β-element subsets of G and let G act on X by left multiplication. Now

This is a group action; the previous proof carries over without change.

$$\begin{aligned} |X| = {}^{p^\alpha z}C_{p^\beta} &= \frac{(p^\alpha z - 0) \times (p^\alpha z - 1) \times \cdots \times (p^\alpha z - (p^\beta - 1))}{(p^\beta - 0) \times (p^\beta - 1) \times \cdots \times 1} \\ &= \frac{(p^\alpha z - 0) \times (p^\alpha z - 1) \times \cdots \times (p^\alpha z - (p^\beta - 1))}{(p^\beta - 0) \times (p^\beta - 1) \times \cdots \times (p^\beta - (p^\beta - 1))}. \end{aligned}$$

Each term in the numerator is of the form

$$p^\alpha z - k,$$

where k runs from 0 to $p^\beta - 1$. Equally, each corresponding term in the denominator is of the form

$$p^\beta - k,$$

where k runs from 0 to $p^\beta - 1$.

For all terms except the first, in either numerator or denominator, a term will be divisible by a given power of p if, and only if, k is divisible by that power of p, by the solution to Exercise 1.5. In each such case, the highest power of p dividing corresponding terms in the numerator and denominator will be precisely the same, namely the highest power that divides k.

Once we have cancelled all these powers of p, the only remaining power of p in ${}^{p^\alpha z}C_{p^\beta}$ arises from the first terms, p^α in the numerator and p^β in the denominator. Hence the power of p dividing $|X|$ is

$$\frac{p^\alpha}{p^\beta} = p^{\alpha-\beta}$$

as claimed. Thus, we may write $|X| = p^{\alpha-\beta}y$, where y is not divisible by p.

Now, as with the first two Sylow Theorems, we consider the partition equation for the action of G on X defined by left multiplication.

Suppose that the distinct orbits are $\mathrm{Orb}(A_1), \ldots, \mathrm{Orb}(A_s)$. Then the partition equation gives

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|.$$

There must be a term on the right-hand side divisible by a power of p that is at most $p^{\alpha-\beta}$, because, if not, all would be divisible by a higher power, contradicting what we have just proved about $|X|$.

Let A be an orbit whose size is divisible by at most $p^{\alpha-\beta}$. By the Orbit–Stabiliser Theorem, we have

$$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

Consider the powers of p on both sides. On the left we have p^α. The first term on the right contributes *at most* $p^{\alpha-\beta}$. It follows that $|\mathrm{Stab}(A)|$ must contribute at least p^β. Hence

$$|\mathrm{Stab}(A)| \geq p^\beta.$$

As before, we now look at the connection between $\mathrm{Stab}(A)$ and A.

By Lemma 1.4 of this chapter, $|\mathrm{Stab}(A)|$ divides $|A|$. Hence $|\mathrm{Stab}(A)| \leq |A| = p^\beta$.

This second inequality completes the proof that $|\mathrm{Stab}(A)| = p^\beta$ and we have produced the subgroup $\mathrm{Stab}(A)$ of order p^β whose existence was claimed.

We have proved a little more along the way. We started by assuming that $|\mathrm{Orb}(A)|$ was divisible by *at most* $p^{\alpha-\beta}$. We then showed that $|\mathrm{Stab}(A)|$ was precisely p^β. The relation

$$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|$$

now shows that $|\mathrm{Orb}(A)|$ is divisible by precisely $p^{\alpha-\beta}$. In fact, we have

$$|\mathrm{Orb}(A)| = p^{\alpha-\beta}z.$$

Also by Lemma 1.4, we know that $\mathrm{Stab}(A_i)$ is a p-group of order p^γ, where $0 \leq \gamma \leq \alpha$, for any $A_i \in X$. Therefore, by the Orbit–Stabiliser Theorem, $|\mathrm{Orb}(A_i)| = p^{\alpha-\gamma}z$, and so the sizes of all orbits are divisible by z. Furthermore,

$$|\mathrm{Stab}(A_i)| \text{ divides } |A_i|,$$

so $\gamma \leq \beta$, and hence $p^{\alpha-\gamma} \geq p^{\alpha-\beta}$.

As in the Sylow proof, the orbits consist of cosets, only one of which can be a subgroup.

Now assume that there are m subgroups of order p^β. As in the proof of Sylow's Second Theorem, each orbit whose size is divisible by precisely $p^{\alpha-\beta}$ contains exactly one subgroup of order p^β. Let these orbits be $\mathrm{Orb}(A_1)$ up to $\mathrm{Orb}(A_m)$. The remaining orbits have sizes divisible by z and a power of p greater than $p^{\alpha-\beta}$, and hence are divisible by $p^{\alpha-\beta+1}z$.

Gathering terms in the partition equation gives

$$|X| = p^{\alpha-\beta}y = mp^{\alpha-\beta}z + (\text{terms divisible by } p^{\alpha-\beta+1}z).$$

Dividing by $p^{\alpha-\beta}$ gives

$$y = mz + kpz$$

for some positive integer k that depends on the particular group of order $p^\alpha z$.

We now do the same as in the proof of Sylow's Second Theorem and apply this result to the cyclic group $\mathbb{Z}_{p^\alpha z}$, of order $p^\alpha z$, for which we know that the corresponding value of m is 1. That is, $y = 1 \times z + k'pz$, for some (other) positive integer k'.

A cyclic group has a unique subgroup corresponding to each divisor of its order.

Equating the two expressions for y gives

$$mz + kpz = z + k'pz.$$

Dividing by z gives

$$m + kp = 1 + k'p.$$

Lastly, reducing modulo p gives

$$m \equiv 1 \,(\text{mod } p).$$

This completes the proof. ■

Theorem 3.1 provides additional restrictions on the number of subgroups of a particular order that a group may possess. These restrictions may be useful when classifying groups of a particular order.

Although we cannot say that two subgroups of a particular prime power order must be conjugate, we can rescue part of Sylow's Third Theorem. Any conjugate of a subgroup of order p^β is also a subgroup of order p^β. If we can show that such a subgroup is unique ($m = 1$), then we can deduce that it is equal to all its conjugates, hence that is normal. However, in the absence of coprimeness, uniqueness is usually hard to prove.

Exercise 3.3

Show that any group of order 196 has a normal subgroup of order 49. Give an example of a group of order 196 that has more than one subgroup of order 7.

This concludes our investigation of subgroups of prime power orders.

4 Groups of order $2p^2$

In this last section of Book B, you will work through a series of exercises that lead to the classification of groups of order $2p^2$, where p is an odd prime. Part of the purpose of this is to pull together various results from the book. Many of the exercises are about applying results that have already been proved, so we suggest that you approach each exercise by first checking for relevant results that might help.

We start with a useful result about direct products.

Exercise 4.1

Let G be a finite group with two subgroups H and K satisfying the following:

1. $H \cap K = \{e\}$
2. $|H||K| = |G|$
3. K is contained in the centre of G.

Show that $G = H \times K$.

Exercise 4.2

Let G and H be finite groups with $|G| = |H|$ and let $\phi : G \to H$ be a homomorphism from G to H. Show that if ϕ is one–one then ϕ is an isomorphism.

An isomorphism from a group to itself is known as an **automorphism**. The next exercise investigates certain automorphisms of cyclic groups of order p^2, where p is an odd prime.

Exercise 4.3

Let $H \cong \mathbb{Z}_{p^2}$, where p is an odd prime number, and let $\phi : H \to H$ be an automorphism of H such that ϕ^2 is the identity.

Show that either ϕ is the identity, or

$$\phi(h) = h^{-1} \quad \text{for all } h \in H.$$

Hint: consider the effect of ϕ on a generator of H.

Exercise 4.4

Let G be a group of order $2p^2$, where p is an odd prime. Let H be a Sylow p-subgroup of G.

(a) Show that H is normal in G. To how many different (up to isomorphism) groups might H be isomorphic? Describe each of these groups.

(b) Let $x \in G$ with $x \notin H$. By considering the natural homomorphism $\theta : G \to G/H$, show that x cannot have order p.

(c) Explain why G has an element a of order 2. Show that the map $\phi : H \to G$ defined by

$$\phi : h \mapsto aha$$

is an automorphism of H.

(d) Show that $G = \{ah : h \in H\} \cup H$. For $h_1, h_2 \in H$, write ah_1ah_2 as an expression involving h_1, h_2 and the automorphism ϕ from part (c).

(e) Show that if $H \cong \mathbb{Z}_{p^2}$ then either $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$ or $G \cong D_{p^2}$.

(f) Show that G has either $1, p$ or p^2 elements of order 2.

(g) If G has exactly one element of order 2, show that G is abelian and list the possible groups to which G can be isomorphic.

(h) Show that if G has p elements of order 2, then $G \cong D_p \times \mathbb{Z}_p$.

(i) Show that if $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and G has p^2 elements of order 2, then G is uniquely determined up to isomorphism.

The solution to Exercise 4.4 shows that a group of order $2p^2$ is isomorphic to one of:

- $\mathbb{Z}_{2p^2}$
- $\mathbb{Z}_{2p} \times \mathbb{Z}_p$
- $D_p \times \mathbb{Z}_p$
- the group described in part (i) of the exercise.

In other words, we have obtained a classification for the groups of order $2p^2$, where p is an odd prime. The group described in part (i) is an example of a structure known as a *semidirect product*. In the case $p = 3$, so that we are considering groups of order 18, this structure is the subgroup of S_6 generated by $(1\,2\,3), (4\,5\,6)$ and $(1\,3)(4\,6)$: the 3-cycles $(1\,2\,3)$ and $(4\,5\,6)$ generate the $\mathbb{Z}_3 \times \mathbb{Z}_3$ subgroup, and $(1\,3)(4\,6)$ is the element a of order 2.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Apply the Sylow Theorems to make deductions about the existence of subgroups of certain orders.

(b) Apply the Sylow Theorems to the classification of groups of a particular order (in simple cases).

(c) Apply counting arguments based on group actions to simple cases.

(d) List all possible abelian groups of a given finite order.

(e) Follow the style of proof used in proving the Sylow Theorems.

Solutions to exercises

Solution to Exercise 1.1

Let G be any group of order 20. Let X be the set of all five-element subsets of G and define an action of G on X by

$$g \wedge A = gA$$

for every element A of X.

The number of five-element subsets of G is

$$\begin{aligned} {}^{20}C_5 &= \frac{20 \times 19 \times 18 \times 17 \times 16}{5 \times 4 \times 3 \times 2 \times 1} \\ &= \frac{4 \times 19 \times 6 \times 17 \times 16}{1 \times 4 \times 1 \times 2 \times 1} \\ &= 19 \times 6 \times 17 \times 8 \\ &= 15504. \end{aligned}$$

Thus $|X| = 15504$.

In Example 1.3, the significant fact about $|X|$ was that it was not divisible by the prime being considered (2 in the example). Here, $|X| = 15504$ is not divisible by 5.

Suppose that

$$\mathrm{Orb}(A_1), \mathrm{Orb}(A_2), \ldots, \mathrm{Orb}(A_s)$$

are the distinct orbits for this group action. Then

$$15504 = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|.$$

If all the terms on the right-hand side were divisible by 5, then so would be the left-hand side. It follows that at least one term on the right-hand side is not divisible by 5.

Suppose that A is an element of X such that $|\mathrm{Orb}(A)|$ is not divisible by 5. The Orbit–Stabiliser Theorem gives

$$20 = |G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

Since $|\mathrm{Orb}(A)|$ is not divisible by 5, $|\mathrm{Stab}(A)|$ must be. Hence

$$|\mathrm{Stab}(A)| \geq 5.$$

As in the example, we now derive the opposite inequality.

If g is any element of $\mathrm{Stab}(A)$ then

$$g \wedge A = gA = A.$$

Thus, for a fixed element a of A, we have $ga \in A$, for all elements g of $\mathrm{Stab}(A)$. Hence the whole of the right coset

$$\mathrm{Stab}(A)a \subseteq A.$$

Thus, because a right coset has the same number of elements as the subgroup from which it is formed,

$$|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq |A| = 5.$$

Hence $|\mathrm{Stab}(A)| = 5$ and $\mathrm{Stab}(A)$ is a subgroup of G of order 5.

Solution to Exercise 1.2

We have to show that if A is a subset of G with k elements, then so is gA. Since gA consists of products of elements of G, by closure it is a subset of G.

We show that gA has k elements by showing that the function from A to gA defined by

$$a \mapsto ga$$

is one–one and onto.

Suppose that $ga_1 = ga_2$. Then, by left cancellation, $a_1 = a_2$. Hence the function is one–one.

Since every element of gA is of the form ga for some element a of A, the function is onto.

Thus A and gA have the same number of elements, k, and so $g \wedge A = gA \in X$. We now check that $\wedge$ satisfies the conditions in the definition of a group action.

(a) We have $e \wedge A = eA = \{ea : a \in A\} = \{a : a \in A\} = A$.

(b) By the definition of $\wedge$ and associativity in G, if g and h are elements of G, we have

$$\begin{aligned}(gh) \wedge A &= (gh)A \\ &= \{(gh)a : a \in A\} \\ &= \{g(ha) : a \in A\} \\ &= g \wedge \{ha : a \in A\} \\ &= g \wedge (hA) \\ &= g \wedge (h \wedge A).\end{aligned}$$

Solution to Exercise 1.3

(a) The highest power of 3 that divides 24 is $3^1 = 3$. Also

$$\begin{aligned}{}^{24}C_3 &= \frac{24 \times 23 \times 22}{3 \times 2 \times 1} \\ &= \frac{8 \times 23 \times 22}{1 \times 2 \times 1} \\ &= 8 \times 23 \times 11 \ (= 2024),\end{aligned}$$

which is not divisible by 3. This fills in the gap in the generalisation of Example 1.3, and we may deduce that any group of order 24 has a subgroup of order 3.

(b) The highest power of 2 dividing 24 is $2^3 = 8$. We have

$$
\begin{aligned}
{}^{24}C_8 &= \frac{24 \times 23 \times 22 \times 21 \times 20 \times 19 \times 18 \times 17}{8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1} \\
&= \frac{3 \times 23 \times 11 \times 21 \times 5 \times 19 \times 9 \times 17}{1 \times 7 \times 3 \times 5 \times 1 \times 3 \times 1 \times 1} \\
&= 23 \times 11 \times 3 \times 19 \times 3 \times 17 \ (= 735471),
\end{aligned}
$$

which is not divisible by 2. As above, we may deduce that every group of order 24 has a subgroup of order 8.

(c) The calculations are slightly shorter here.

$$
\begin{aligned}
{}^{15}C_3 &= \frac{15 \times 14 \times 13}{3 \times 2 \times 1} \\
&= \frac{5 \times 7 \times 13}{1 \times 1 \times 1} \\
&= 5 \times 7 \times 13 \ (= 455),
\end{aligned}
$$

which is not divisible by 3. Hence G has a subgroup H of order 3.

$$
\begin{aligned}
{}^{15}C_5 &= \frac{15 \times 14 \times 13 \times 12 \times 11}{5 \times 4 \times 3 \times 2 \times 1} \\
&= \frac{3 \times 7 \times 13 \times 6 \times 11}{1 \times 2 \times 3 \times 1 \times 1} \\
&= 3 \times 7 \times 13 \times 11 \ (= 3003),
\end{aligned}
$$

which is not divisible by 5. Hence G has a subgroup K of order 5.

Solution to Exercise 1.4

(a) The subgroup that is the intersection of two Sylow 5-subgroups must, by Lagrange's Theorem, have order 1 or 5. Since the subgroups are distinct, the intersection must have order 1 and hence be trivial.

(b) There are m subgroups of order 5, where m is congruent to 1 modulo 5. The possibilities for m are $1, 6, \ldots$. However, by part (a), every new five-element subgroup contributes four more non-identity elements of order 5. Thus, if there were six or more such subgroups, we would have the identity plus at least 24 other elements. Since this is impossible, we conclude that $m = 1$.

This unique Sylow 5-subgroup contains the identity and four elements of order 5. Since any element of order 5 in G would generate a Sylow 5-subgroup, G can have only these four elements of order 5.

(c) By a similar argument to that for order 5 in part (a), any two distinct subgroups of order 3 have trivial intersection. Each such subgroup has two non-identity elements of order 3. Hence there are $2l$ elements of order 3 in G.

(d) Elements of G can only have orders 1, 3, 5 and 15.

The identity is the only element of order 1.

There are four elements of order 5.

There are $2l$ elements of order 3.

If there are no elements of order 15 then we must have

$$15 = 1 + 4 + 2l,$$

which gives $l = 5$. However, 5 is not congruent to 1 modulo 3 as required by Sylow's Second Theorem. This contradiction shows that G must have an element of order 15, and so it is cyclic.

Solution to Exercise 1.5

(a) (i) Suppose that p^β divides $p^\alpha z - k$. Then

$$p^\alpha z - k = p^\beta l$$

for some integer l. Thus

$$k = p^\alpha z - p^\beta l.$$

Suppose now that $\beta \geq \alpha$, so that $p^\beta \geq p^\alpha$. Then

$$\begin{aligned} k &= p^\alpha z - p^\beta l \\ &= p^\alpha (z - p^{\beta-\alpha} l). \end{aligned}$$

Thus p^α divides k, contradicting the fact that $0 < k < p^\alpha$. Hence $\beta < \alpha$ as required.

(ii) Again suppose that p^β divides $p^\alpha z - k$. Then, as above,

$$k = p^\alpha z - p^\beta l$$

for some integer l. By part (i), we have $\beta < \alpha$, so that $p^\alpha > p^\beta$. Therefore

$$\begin{aligned} k &= p^\alpha z - p^\beta l \\ &= p^\beta \big(p^{\alpha-\beta} z - l\big). \end{aligned}$$

Thus p^β divides k.

Conversely, suppose that p^β divides k. Then, as $0 < k < p^\alpha$, we must have $\beta < \alpha$ and so p^β divides p^α. Hence p^β divides both terms in

$$p^\alpha z - k,$$

and therefore divides $p^\alpha z - k$.

(b) Consider the terms in the binomial coefficient

$$\frac{(p^\alpha z - 0) \times (p^\alpha z - 1) \times \cdots \times (p^\alpha z - (p^\alpha - 1))}{(p^\alpha - 0) \times (p^\alpha - 1) \times \cdots \times (p^\alpha - (p^\alpha - 1))}.$$

Since p does not divide z, the power of p dividing the first term in the numerator is the same as the power of p dividing the first term in the denominator, namely p^α.

Each remaining term in the numerator is of the form $p^\alpha z - k$ with $0 < k < p^\alpha$. By part (a), the maximum power of p dividing $p^\alpha z - k$ is the maximum power of p dividing k. This is true for all integer values of z. In particular, it is true for the case $z = 1$. Hence, the maximum power of p dividing k is also the maximum power of p dividing $p^\alpha 1 - k = p^\alpha - k$, which is the term in the denominator corresponding to $p^\alpha z - k$ in the numerator.

Hence each factor of p in the numerator is cancelled out by a corresponding factor of p in the denominator.

Thus the binomial coefficient ${}^{p^\alpha z}C_{p^\alpha}$ is not divisible by p.

Solution to Exercise 1.6

(a) Since $91 = 7 \times 13$, the Sylow 13-subgroups of G are of order 13 and hence cyclic. By an argument used in Exercise 1.4, any two distinct subgroups of order 13 will have trivial intersection. Thus each new subgroup of order 13 contributes twelve additional elements of order 13.

If G has m Sylow 13-subgroups, then m is congruent to 1 modulo 13. Thus the possibilities for m are $m = 1, 14, \ldots$. But 14 such subgroups would contain

$$1 + 14 \times 12 = 169$$

distinct elements, a contradiction since $|G| = 91$. Thus $m = 1$.

(b) So far, we know that G has one element of order 1 and twelve of order 13 (in the unique Sylow 13-subgroup). We now show that the remaining 78 elements cannot all be of order 7.

Since $91 = 7 \times 13$, the Sylow 7-subgroups of G must be cyclic and of order 7. As before, any two distinct such subgroups have trivial intersection. Suppose that G has l Sylow 7-subgroups. Each such subgroup accounts for six elements of G of order 7.

Assume that there are no elements of order 91 (the only remaining possible order). Counting the elements of G gives

$$91 = 1 + 12 + 6l,$$

which requires $l = 13$. But 13 is not congruent to 1 modulo 7, contradicting Sylow's Second Theorem.

Thus G has at least one element of order 91 and so it is cyclic.

Solution to Exercise 1.7

(a) Since $|G| = pq$, the Sylow q-subgroups of G are of prime order q and hence cyclic.

As in the solutions to Exercises 1.4 and 1.6, each such subgroup has $q-1$ elements of order q and any two distinct such subgroups have trivial intersection. So each new subgroup of order q contributes $q-1$ additional elements of order q.

If G has m Sylow q-subgroups, then m is congruent to 1 modulo q and so the possibilities for m are $m = 1, q+1, \ldots$. However, $q+1$ such subgroups would contain

$$1 + (q+1)(q-1) = 1 + q^2 - 1 = q^2$$

elements. Since $p < q$, we have

$$|G| = pq < qq = q^2.$$

This contradiction shows that $m = 1$.

Sylow's Third Theorem, which we discuss in the next subsection, provides a shorter proof that the subgroup is unique.

(b) The conjugate of a subgroup is a subgroup having the same order. Since any Sylow q-subgroup H is unique, all conjugates of H must be H itself. That is,

$$gHg^{-1} = H, \quad \text{for all } g \in G,$$

and so H is normal in G.

Solution to Exercise 1.8

First of all, we see that $h \wedge (gK) = (hg)K \in X$ for all $g \in G$ and all $h \in H$, so that $\wedge$ indeed defines a function from $H \times X$ to X. We check that this function satisfies the properties in Definition 3.1 of Chapter 6.

(a) $e \wedge (gK) = (eg)K = gK$ for all $g \in G$.

(b) If $h_1, h_2 \in H$ then
$h_1 \wedge (h_2 \wedge (gK)) = h_1 \wedge (h_2 gK) = (h_1 h_2 gK) = (h_1 h_2) \wedge gK$.

Solution to Exercise 1.9

(a) Since $|K| = p^\alpha$, Lagrange's Theorem implies that $|X| = z$.

(b) From the Orbit–Stabiliser Theorem,

$$|H| = |\mathrm{Orb}(gK)| \times |\mathrm{Stab}(gK)|.$$

The result $|\mathrm{Orb}(gK)| = p^\beta$ follows from $|H| = p^\alpha$.

(c) Suppose that this action has s distinct orbits. Then the partition equation gives

$$\begin{aligned} z = |X| &= |\mathrm{Orb}(g_1K)| + |\mathrm{Orb}(g_2K)| + \cdots + |\mathrm{Orb}(g_sK)| \\ &= p^{\beta_1} + p^{\beta_2} + \cdots + p^{\beta_s}. \end{aligned}$$

Since z is not divisible by p, there must be at least one $\beta_i = 0$, that is, $|\mathrm{Orb}(g_iK)| = 1$. Then g_i is the required a.

(d) From part (c), we know there is $a \in G$ such that $|\mathrm{Orb}(aK)| = 1$. Then for all $h \in H$ we have $h \wedge (aK) = aK$, that is,

$$(ha)K = aK.$$

This tells us that $a^{-1}(ha)K = K$, so $a^{-1}ha \in K$. Since this holds for all $h \in H$, we have

$$a^{-1}Ha \subseteq K.$$

But $|H| = |K| = p^\alpha$, and $|a^{-1}Ha| = |K|$, therefore $a^{-1}Ha = K$ and so H and K are conjugate, as required.

Solution to Exercise 1.10

(a) Since the conjugate of a Sylow p-subgroup is again a Sylow p-subgroup, we have that

$$g \wedge H_i = gH_ig^{-1}$$

for all $g \in G$ and H_i in X. Therefore $\wedge$ defines a function from $G \times X$ to X. We check that the properties in Definition 3.1 of Chapter 6 hold.

(i) Since $eH_ie^{-1} = eH_ie = H_i$, we have $e \wedge H_i = H_i$ for all $H_i \in X$.

(ii) Let $g_1, g_2 \in G$. Then

$$\begin{aligned} g_1 \wedge (g_2 \wedge H_i) &= g_1 \wedge (g_2H_ig_2^{-1}) \\ &= g_1(g_2H_ig_2^{-1})g_1^{-1} \\ &= (g_1g_2)H_i(g_1g_2)^{-1} \\ &= (g_1g_2) \wedge H_i. \end{aligned}$$

(b) From Exercise 1.9, we know that all Sylow p-subgroups are conjugate. This means there is only one orbit.

(c) Since there is only one orbit, we know $|\mathrm{Orb}(H_1)| = |X| = m$, so the Orbit–Stabiliser Theorem gives

$$|G| = |\mathrm{Orb}(H_1)| \times |\mathrm{Stab}(H_1)| = m \times |\mathrm{Stab}(H_1)|.$$

Solution to Exercise 1.11

(a) We know that l is congruent to 1 modulo 3 and that l divides 5. The first requirement gives $l = 1, 4, 7, \ldots$, and the only one of these values satisfying the second restriction is $l = 1$.

(b) We know that m is congruent to 1 modulo 5 and that m divides 3. The first requirement gives $m = 1, 6, 11, \ldots$, and the only one of these values satisfying the second restriction is $m = 1$.

(c) We now know that G contains the identity, just four elements of order 5 and just two elements of order 3. The remaining eight elements must, therefore, have order 15 (the only remaining possible order). Hence G is cyclic.

Solution to Exercise 1.12

Suppose that G has l Sylow 3-subgroups. Then l is congruent to 1 modulo 3, that is, $l = 1, 4, 7, \ldots$. Among these possible values for l, only 1 divides 2. Hence G has a unique Sylow 3-subgroup.

Suppose that G has m Sylow 2-subgroups. Then m is congruent to 1 modulo 2. So $m = 1, 3, 5, \ldots$, of which both 1 and 3 divide 3. Hence G could have one or three Sylow 2-subgroups.

There are only two different groups of order 6, namely $\mathbb{Z}_6$ and S_3.

Since $\mathbb{Z}_6$ is cyclic, it has a unique subgroup corresponding to each divisor of its order. Thus, $\mathbb{Z}_6$ has one Sylow 2-subgroup.

In S_3, each of the 2-cycles $(1\,2), (1\,3)$ and $(2\,3)$ generates a distinct subgroup of order 2. Hence S_3 has three Sylow 2-subgroups.

Solution to Exercise 2.1

Let G be an abelian group of order 72. Since $72 = 8 \times 9 = 2^3 \times 3^2$, by Theorem 2.2 we have $G \cong H \times K$, where H has order 8 and K has order 9.

The possibilities for H are

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

and the possibilities for K are

$$\mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3.$$

It follows that G is one of

- $\mathbb{Z}_8 \times \mathbb{Z}_9 (\cong \mathbb{Z}_{72})$
- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 (\cong \mathbb{Z}_{24} \times \mathbb{Z}_3)$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 (\cong \mathbb{Z}_{36} \times \mathbb{Z}_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_{18})$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 (\cong \mathbb{Z}_{12} \times \mathbb{Z}_6)$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 (\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18})$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 (\cong \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2)$.

Therefore there are six abelian groups of order 72 up to isomorphism.

Solution to Exercise 2.2

(a) Firstly, since $\mathbb{Z}_6$ is abelian, there is a normal Sylow subgroup for each prime divisor. The conjugacy part of Sylow's Third Theorem, together with normality, tells us that this subgroup is unique.

Since $|\mathbb{Z}_6| = 2 \times 3$, the Sylow 2-subgroup has order 2, hence it is (isomorphic to) $\mathbb{Z}_2$. Similarly, the Sylow 3-subgroup is $\mathbb{Z}_3$.

In terms of the elements of $\mathbb{Z}_6$, the subgroups are

$$\{0, 3\} \quad \text{and} \quad \{0, 2, 4\}.$$

(b) Since the group is abelian, the argument about uniqueness of Sylow p-subgroups given in part (a) holds here too. The group has order

$$3 \times 15 = 3^2 \times 5.$$

Since 3 and 5 are coprime, we know that $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$, so

$$\mathbb{Z}_3 \times \mathbb{Z}_{15} \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5.$$

Thus the Sylow 3-subgroup (of order 3^2) is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$ and the Sylow 5-subgroup (of order 5) is isomorphic to $\mathbb{Z}_5$.

As a subgroup of $\mathbb{Z}_3 \times \mathbb{Z}_{15}$, the Sylow 3-subgroup is

$$\mathbb{Z}_3 \times \{0, 5, 10\}.$$

Similarly, the Sylow 5-subgroup is

$$\{0\} \times \{0, 3, 6, 9, 12\}.$$

(c) The order of S_3 is $6 = 2 \times 3$. Since S_3 is not abelian, we cannot argue as above that the Sylow subgroups are unique.

However, the Sylow 3-subgroup is unique, for the following reasons. If there are m Sylow 3-subgroups, then we know that

$$m \equiv 1 \,(\mathrm{mod}\ 3) \quad \text{and} \quad m \mid 2.$$

The only solution is $m = 1$.

We can also derive this result from knowledge of the elements of S_3. Any Sylow 3-subgroup must be cyclic and of order 3. There are only two elements of order 3, namely the 3-cycles

$$(1\,2\,3) \quad \text{and} \quad (1\,3\,2).$$

Thus the only possibility for a Sylow 3-subgroup is

$$\{e, (1\,2\,3), (1\,3\,2)\}.$$

Since this is a subgroup, it must be the unique Sylow 3-subgroup.

Any Sylow 2-subgroup must be cyclic and of order 2. There are three elements of order 2, the 2-cycles

$$(1\,2), \quad (1\,3) \quad \text{and} \quad (2\,3).$$

Each 2-cycle generates a cyclic subgroup of order 2, so the Sylow 2-subgroups are

$$\{e, (1\,2)\}, \quad \{e, (1\,3)\} \quad \text{and} \quad \{e, (2\,3)\}.$$

The number of Sylow 2-subgroups is 3. As a check,

$$3 \equiv 1 \,(\mathrm{mod}\ 2) \quad \text{and} \quad 3 \mid 6.$$

Note that, as expected from the theory, all the Sylow 2-subgroups are conjugate because their generators have the same cycle type and are, therefore, conjugate in S_3.

Solution to Exercise 2.3

(a) There are several perfectly good proofs that D_7 has a unique Sylow 7-subgroup. All use the fact that, since the order of D_7 is $14 = 2 \times 7$, any Sylow 7-subgroup has order 7.

First proof
Any Sylow 7-subgroup must contain a generator of order 7. The only elements of order 7 are the non-trivial rotations. The rotation subgroup contains all such elements, has order 7 and so it must be the unique Sylow 7-subgroup.

Second proof
Any Sylow 7-subgroup has index 2. Therefore it is normal, and hence unique.

Third proof
The number of Sylow 7-subgroups is congruent to 1 modulo 7. Possible numbers are 1, 8, ... Each such subgroup would contribute six 'new' elements of order 7, so eight or more such subgroups are impossible. Thus the Sylow 7-subgroup is unique.

Fourth proof
The number of Sylow 7-subgroups is congruent to 1 modulo 7 and divides 2. The only possibility is 1.

(b) Any Sylow 2-subgroup of D_7 has order 2 and hence it is cyclic. Again, there are several possible proofs that there are seven such subgroups. We give two.

First proof
There are seven reflections in D_7. Each generates a distinct subgroup of order 2, which is a Sylow 2-subgroup. There are no other elements of order 2.

Second proof
The number of Sylow 2-subgroups is congruent to 1 modulo 2, that is, it is odd, and divides 7. The possibilities are 1 and 7.

Suppose there is a unique Sylow 2-subgroup. We count the elements of various orders. There is only one element of order 1. There are six elements of order 7 in the unique Sylow 7-subgroup. By our assumption, there is only one element of order 2. We have accounted for only eight elements of G. Hence the remaining elements must have order 14 (the only other possible order). This forces

$$D_7 \cong \mathbb{Z}_{14},$$

a contradiction because $\mathbb{Z}_{14}$ is abelian and D_7 is not.

The only remaining possibility is that there are seven Sylow 2-subgroups.

(c) In a Sylow 2-subgroup, each reflection is the non-identity element. As all such subgroups are conjugate and the identity always conjugates to itself, the result follows.

(d) Using the notation of the presentation, the non-identity rotations are

$$a, a^2, a^3, a^4, a^5, a^6.$$

Conjugating a^i by another rotation a^j gives

$$a^j a^i a^{-j} = a^{j+i-j} = a^i.$$

Conjugating by a reflection $a^j b$ gives

$$\begin{aligned}(a^j b)a^i(a^j b)^{-1} &= a^j(ba^i)b^{-1}a^{-j} \\ &= a^j a^{-i} b b^{-1} a^{-j} \qquad (\text{since } ba^i = a^{-i}b) \\ &= a^{j-i-j} \\ &= a^{-i}.\end{aligned}$$

Thus every conjugate of a rotation is either itself or its inverse.

(e) The various calculations above show that the conjugacy classes in D_7 are

$$\{e\},\ \{b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\},\ \{a, a^6\},\ \{a^2, a^5\},\ \{a^3, a^4\}.$$

The class equation is

$$14 = 1 + 7 + 2 + 2 + 2.$$

The centre consists of the single-element conjugacy classes. Hence the centre of D_7 is the trivial subgroup $\{e\}$.

Solution to Exercise 2.4

We already know, from our work on abelian groups, that there is only one abelian group of order 14, namely $\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$.

Let G be any group of order 14.

By the Sylow Theorems, there is a unique (normal) Sylow 7-subgroup, which must be cyclic and of order 7. Let this subgroup be

$$\langle a \mid a^7 = e \rangle.$$

Again by the Sylow Theorems, there is at least one Sylow 2-subgroup – in fact, there are either one or seven Sylow 2-subgroups. Let

$$\langle b \mid b^2 = e \rangle$$

be one such subgroup.

Because b has order 2, it is not an element of $\langle a \rangle$. Therefore the cosets

$$\begin{aligned}\langle a \rangle &= \{e, a, a^2, a^3, a^4, a^5, a^6\} \qquad \text{and} \\ \langle a \rangle b &= \{b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\}\end{aligned}$$

are distinct and give all 14 elements of G. In particular, a and b generate G.

We now have most of the ingredients for a presentation of D_7. All that is left to do is to show that $ba = a^{-1}b$, or equivalently that $bab^{-1} = a^{-1}$.

The element bab^{-1} is a conjugate of a and so, as you can easily check, has order 7 (remember that conjugate elements always have the same order).

It therefore belongs to the unique subgroup of order 7 generated by a. Hence

$$bab^{-1} = a^i \quad \text{for some integer } i \in \{1, 2, \ldots, 6\}.$$

Note that as bab^{-1} has order 7, it cannot be the identity, which excludes $i = 0$.

Conjugating again by b gives

$$\begin{aligned} b^2ab^{-2} &= b(bab^{-1})b^{-1} \\ &= ba^ib^{-1} \\ &= (bab^{-1})^i \\ &= (a^i)^i \\ &= a^{i^2}. \end{aligned}$$

Since $b^2 = e$, this gives $a = a^{i^2}$. So, as a has order 7, $i^2 \equiv 1 \,(\text{mod } 7)$ and, by exhaustion, $i = 1$ or 6.

If $i = 1$ then a and b commute. Since a and b generate G, this implies that G is abelian and hence

$$G \cong \mathbb{Z}_{14}.$$

We are left with the case $i = 6$, that is, $bab^{-1} = a^6 = a^{-1}$. So in this case

$$G \cong \langle a, b \mid a^7 = e,\ b^2 = e,\ ba = a^6b\,(= a^{-1}b)\rangle = D_7.$$

Solution to Exercise 2.5

Since the order of D_{14} is $28 = 2^2 \times 7$, the Sylow subgroups have orders 4 and 7. Any Sylow 7-subgroup must be cyclic. A Sylow 2-subgroup is either cyclic or the Klein group.

(a) The number of Sylow 7-subgroups must be one of 1, 8, ... as well as being a divisor of 4. The only possibility is 1.

(b) The identity e has order 1.

The 14 reflections

$$b, ab, a^2b, \ldots, a^{13}b$$

all have order 2.

The rotations form the subgroup

$$\{e, a, a^2, \ldots, a^{13}\},$$

which is of order 14. Thus, the only possible orders of the non-identity rotations are 2, 7 and 14. From our knowledge of cyclic groups, we know that each of these does occur. For example, a has order 14, a^2 has order 7 and a^7 has order 2.

In fact, the orders of the rotations are as follows.

Order 1: e.
Order 2: a^7.
Order 7: $a^2, a^4, a^6, a^8, a^{10}, a^{12}$.
Order 14: $a, a^3, a^5, a^9, a^{11}, a^{13}$.

So a^7 is the only rotation of order 2.

(c) The most straightforward argument is the direct/indirect symmetry one. Suppose that the 14-gon is coloured red on one side and blue on the other. Since each reflection changes the colour of a 14-gon, the product of two reflections preserves the colour and so is a rotation. Note that this includes the identity rotation, which is produced just in those cases where the two reflections are identical.

Any Sylow 2-subgroup has order 4 and so it can only contain elements of orders 1, 2 and 4. There are no elements of order 4, so each Sylow 2-subgroup contains the identity and three elements of order 2 (so is the Klein group).

There is only one rotation of order 2. Thus at least two elements of a Sylow 2-subgroup are reflections. However, the product of two such *distinct* reflections is a non-identity rotation. Thus each Sylow 2-subgroup contains two distinct reflections and the unique rotation of order 2.

(d) Any conjugate of a^7, the rotation of order 2, must be another rotation of order 2, since conjugation preserves order (Proposition 2.5 of Chapter 5) and maps direct symmetries to direct symmetries. There is only one such rotation, so the subgroup

$$\{e, a^7\}$$

has no conjugate subgroups apart from itself, and hence is normal by Proposition 3.10 of Chapter 5.

Alternatively, the subgroup $\{e, a^7\}$ is a union of conjugacy classes, and hence it is normal by Proposition 3.12 of Chapter 5.

From part (c), $\{e, a^7\}$ lies in every Sylow 2-subgroup.

(e) The number of Sylow 2-subgroups is odd (congruent to 1 modulo 2) and divides 7. Therefore the only possibilities are 1 and 7.

There are several ways to rule out 1, the easiest of which is as follows.

Each Sylow 2-subgroup contains e, a^7 and two 'new' reflections. There are, in all, 14 reflections (of order 2). To account for them requires seven Sylow 2-subgroups.

Solution to Exercise 2.6

(a) We have

$$|G| = 221 = 13 \times 17.$$

The number of Sylow 13-subgroups of G is congruent to 1 modulo 13 and divides 17. Thus there is a unique Sylow 13-subgroup.
The number of Sylow 17-subgroups is congruent to 1 modulo 17 and divides 13. Thus there is a unique Sylow 17-subgroup.

Therefore G has unique, normal, cyclic Sylow subgroups of coprime orders 13 and 17. Hence, by Theorem 2.3 and Theorem 2.11 of Chapter 6,

$$G \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17} \cong \mathbb{Z}_{221},$$

and G is cyclic.

(b) Since $111 = 3 \times 37$, an argument like that in part (a) shows that a group of order 111 must have a unique Sylow 37-subgroup. However, the number of Sylow 3-subgroups can be either 1 or 37, since both are congruent to 1 modulo 3 and both divide 37. We therefore cannot be sure that there is a unique Sylow 3-subgroup.

Solution to Exercise 2.7

The order of G has prime decomposition

$$110 = 2 \times 5 \times 11.$$

We check the number of Sylow subgroups corresponding to 2, 5 and 11 in turn.

For the 2-subgroups, the number must be congruent to 1 modulo 2 and divide 55. Thus there could be 1, 5, 11 or 55 such subgroups.

For the 5-subgroups, the number must be congruent to 1 modulo 5 and divide 22. Thus there could be 1 or 11 such subgroups.

For the 11-subgroups, the number must be congruent to 1 modulo 11 and divide 10. Thus there can only be one such subgroup.

Hence we can be sure that there is a unique Sylow 11-subgroup, which is normal because it is unique. Since it has order 11, this subgroup is non-trivial. Since its order is less than that of the group, it is proper.

Solution to Exercise 2.8

The order factorises into primes as

$$132 = 2^2 \times 3 \times 11.$$

By the usual argument, the possibilities for the numbers of each type of Sylow subgroup are shown in the table below.

Sylow 2-subgroups	1, 3, 11 or 33
Sylow 3-subgroups	1, 4 or 22
Sylow 11-subgroups	1 or 12

We want to rule out the possibility that there is more than one of every Sylow subgroup type. Suppose that we have twelve Sylow 11-subgroups, at least four Sylow 3-subgroups and at least three Sylow 2-subgroups.

Since the Sylow 11-subgroups are cyclic of prime order, the twelve subgroups account for the identity element plus 120 elements of order 11. A similar argument shows that the four Sylow 3-subgroups, which are cyclic, account for eight non-identity elements, each of order 3.

We have accounted for 129 elements of the group: the identity, 120 elements of order 11 and eight elements of order 3. There are only three elements left, and these must be the three non-identity elements of a Sylow 2-subgroup (which has order 4). This contradicts the assumption

that there are at least three Sylow 2-subgroups. Thus at least one Sylow subgroup must be unique and hence normal, and so G is not simple.

Solution to Exercise 3.1

(a) From the presentation, we know that a has order 4, so

$$\langle a \rangle \cong \mathbb{Z}_4$$

is a cyclic subgroup of order 4.

(b) Let $H = \{e, a^2, b, a^2b\}$.

Closure is almost immediate. Probably the only combinations needing more than a mental check are the following:

$$\begin{aligned} ba^2 &= (a^3)^2 b \qquad \text{(since } ba = a^3b\text{)} \\ &= a^6 b \\ &= a^2 b; \end{aligned}$$

$$\begin{aligned} ba^2b &= (a^2b)b \qquad \text{(by the above)} \\ &= a^2b^2 \\ &= a^2; \end{aligned}$$

$$\begin{aligned} a^2ba^2 &= a^2(a^2b) \qquad \text{(by the above)} \\ &= a^4 b \\ &= b. \end{aligned}$$

The identity element is in H and each element is self-inverse (see below). Thus H is a subgroup.

The element a^2 is a half-turn, while the other two non-identity elements are reflections. Hence all non-identity elements are of order 2, so H must be isomorphic to the Klein group.

Solution to Exercise 3.2

(a) We have

$$\begin{aligned} |X| &= \frac{24 \times 23 \times 22 \times 21}{4 \times 3 \times 2 \times 1} \\ &= \frac{6 \times 23 \times 11 \times 21}{1 \times 3 \times 1 \times 1} \\ &= 2 \times 23 \times 11 \times 21 \, (= 10626). \end{aligned}$$

(b) From the factorisation in part (a), we can see that the highest power of 2 that divides $|X|$ is $2^1 = 2$.

(c) This time we have

$$\begin{aligned} |Y| &= \frac{24 \times 23}{2 \times 1} \\ &= 12 \times 23 \, (= 276). \end{aligned}$$

(d) The highest power of 2 that divides $|Y|$ is 2^2.

Solution to Exercise 3.3

We have $196 = 2^2 \times 7^2$. Thus the group has subgroups of order 7 and $7^2 = 49$.

Suppose that there are m subgroups of order 49. Then

$$m \equiv 1 \,(\mathrm{mod}\ 7) \quad \text{and} \quad m \mid 4.$$

Hence $m = 1$, so the Sylow 7-subgroup, of order 49, is unique and, hence, normal.

The abelian group $\mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_7$ has distinct subgroups

$$\{0\} \times \mathbb{Z}_7 \times \{0\} \quad \text{and} \quad \{0\} \times \{0\} \times \mathbb{Z}_7,$$

both of which have order 7.

Solution to Exercise 4.1

Since K is contained in the centre of G, we know that

$$kg = gk$$

for all $k \in K, g \in G$. In particular, $kh = hk$ for all $k \in K$ and $h \in H$, so we can apply Proposition 1.9(b) of Chapter 6 to conclude that HK is a subgroup of G and that

$$HK \cong H \times K.$$

Then Proposition 1.9(a) tells us that $|HK| = |H||K|$; hence, by condition 2, we have that

$$|G| = |HK|.$$

It follows that $G = HK$, hence $G \cong H \times K$ as required.

Solution to Exercise 4.2

If ϕ is a one–one homomorphism, to show that it is an isomorphism we just need to show that ϕ is onto.

Since ϕ is one–one, we know that

$$\phi(g_1) = \phi(g_2) \Rightarrow g_1 = g_2$$

for all $g_1, g_2 \in G$. Thus

$$|\{\phi(g) : g \in G\}| = |G| = |H|.$$

As $\{\phi(g) : g \in G\} \subseteq H$, this means that $\{\phi(g) : g \in G\} = H$ and so ϕ is onto as required.

Solution to Exercise 4.3

Let h be a generator of H, so $H = \langle h \rangle$ and h has order p^2. Then $\phi(h) = h^r$ for some integer r with $0 \leq r < p^2$.

Since ϕ^2 is the identity, we have that

$$h = \phi^2(h) = \phi(\phi(h)) = \phi(h^r) = [\phi(h)]^r = (h^r)^r = h^{r^2}.$$

Thus $h^{r^2-1} = e$ and, since $|h| = p^2$, we have that p^2 divides

$$r^2 - 1 = (r-1)(r+1).$$

It follows that p divides $r^2 - 1 = (r-1)(r+1)$ and, since p is prime, that either p divides $r-1$ or p divides $r+1$.

Suppose that p divides $r-1$. Then p does not divide $r+1$ (as p is an odd prime) and so neither does p^2. By Euclid's Lemma (Book A, Chapter 1, Theorem 4.12), we have that p^2 divides $r-1$. Then

$$r = kp^2 + 1 \quad \text{for some } k \in \mathbb{Z}.$$

The condition $0 \leq r < p^2$ forces $k = 0$, so $r = 1$, and therefore $\phi(h) = h$. Since h generates H, it follows that ϕ is the identity on H.

Now suppose that p divides $r+1$. Then p^2 divides $r+1$, again by Euclid's Lemma, so

$$r = kp^2 - 1 \quad \text{for some } k \in \mathbb{Z}.$$

Now the condition $0 \leq r < p^2$ forces $k = 1$, so that $r = p^2 - 1$. Since h has order p^2,

$$\phi(h) = h^{p^2-1} = h^{-1}.$$

Let $g \in H$. Since h generates H, we have $g = h^s$ for some $s \in \mathbb{Z}$, so

$$\phi(g) = \phi(h^s) = [\phi(h)]^s = (h^{-1})^s = h^{-s} = g^{-1}.$$

Solution to Exercise 4.4

(a) By Sylow's First Theorem, the subgroup H has order p^2. Then H has index 2 in G, and so it is normal (see Exercise 3.3(b) of Chapter 5).

Since H has order p^2, it is abelian by Theorem 2.15 of Chapter 7. Thus by Theorem 3.19 of Chapter 6, either $H \cong \mathbb{Z}_{p^2}$ or $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

(b) Since H is normal in G, we have $|G/H| = 2$. The natural homomorphism $\theta\colon G \to G/H$ is defined by

$$g \mapsto gH \quad \text{for all } g \in G.$$

Let $x \in G$ and $x \notin H$. Then $\theta(x) \neq H$, otherwise we would have $xH = H$, that is $x \in H$. Therefore $\theta(x)$ does not have order 1, so it has order 2.

By Exercise 4.11(b) of Chapter 5, the order of $\theta(x)$ divides the order of x and so, as p is an odd prime, x cannot have order p.

(c) Since 2 is prime and divides the order of G, by Sylow's First Theorem we know that G has at least one Sylow 2-subgroup. As 2^n does not divide $|G|$ for $n \geq 2$, this subgroup must have order 2 and thus it is isomorphic to $\mathbb{Z}_2$. The non-identity element a in this subgroup has order 2. Thus $a^{-1} = a$.

Since H is normal in G, for $h \in H$ we have

$$\phi(h) = aha = aha^{-1} \in H,$$

so the image set of H under ϕ is H itself.

Next note that for any $h_1, h_2 \in H$,

$$\phi(h_1h_2) = ah_1h_2a = ah_1aah_2a = \phi(h_1)\phi(h_2).$$

This shows that ϕ is a homomorphism.

To see that ϕ is one–one, let $h_1, h_2 \in H$ be such that $\phi(h_1) = \phi(h_2)$. Then

$$\phi(h_1) = \phi(h_2) \Rightarrow ah_1a = ah_2a \Rightarrow h_1 = h_2.$$

The solution to Exercise 4.2 and the fact that $\phi(H) = H$ ensure that ϕ is onto H, and so it is an automorphism of H.

(d) Since H has index 2, it has two cosets. Since $a \notin H$, the two cosets are H and aH. Thus $G = aH \cup H$. For $h_1, h_2 \in H$, we have

$$ah_1ah_2 = ah_1\phi(h_2)a = \phi(h_1\phi(h_2)).$$

(e) Let ϕ be the homomorphism defined in part (c), and observe that for all $h \in H$,

$$\phi^2(h) = \phi(aha) = a^2ha^2 = h.$$

Therefore ϕ^2 is the identity map on H. By the solution to Exercise 4.3, the automorphism $\phi : H \to H$ satisfies either $\phi(h) = h$ for all $h \in H$ or $\phi(h) = h^{-1}$ for all $h \in H$.

If $\phi(h) = h$ for all $h \in H$, then $aha = h$ for all $h \in H$. We know from part (d) that $G = aH \cup H$, so this implies that G is abelian. Then Theorem 2.2 gives $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$. Since p is an odd prime, Theorem 2.11 of Chapter 6 gives $G \cong \mathbb{Z}_{2p^2}$.

If G is not abelian then G has presentation

$$G = \langle a, h \mid a^2 = e, h^{p^2} = e, aha = h^{-1} \rangle,$$

so $G \cong D_{p^2}$.

(f) By the Sylow Theorems (Theorem 1.12), the number of Sylow 2-subgroups is odd and divides $2p^2$. Thus there are $1, p$ or p^2 subgroups of order 2.

The required result follows since each Sylow 2-subgroup contains exactly one element of order 2.

(g) If G has exactly one element of order 2, then there is a unique Sylow 2-subgroup K, say, and this is normal.

Since p is an odd prime, $K \cap H = \{e\}$. Now both H and K are normal subgroups of G. Moreover $|H||K| = |G|$, so $G = HK$. Then Theorem 1.5 of Chapter 6 gives

$$G \cong H \times K.$$

Since H and K are abelian, so is G by Exercise 1.4 of Chapter 6. Thus G is isomorphic to one of $\mathbb{Z}_{2p} \times \mathbb{Z}_p$ and $\mathbb{Z}_{2p^2}$.

(h) Suppose that G has p elements of order 2.

If $H \cong \mathbb{Z}_{p^2}$ then, by part (e), either $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$ or $G \cong D_{p^2}$.

If $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$ we know G has one element of order 2. If $G \cong D_{p^2}$, we know G has p^2 elements of order 2 (corresponding to the reflections). Both cases contradict the assumption that G has p elements of order 2. It follows that $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Note that this means that all non-identity elements of H have order p.

Let $a \in G$ with $a^2 = e$. Then $G = H \cup aH$ by part (d). Since no elements of H have order 2, there is $h \in H,\ h \neq e$ such that $(ah)^2 = e$. Then

$$aha = h^{-1}.$$

Let K be the subgroup of G generated by a and h. Then

$$K = \{a^m h^n : a^2 = e, h^p = e, aha = h^{-1}\};$$

that is, $K \cong D_p$.

Let $g \in H$ but $g \notin \langle h \rangle$. Then $\langle g \rangle$ and $\langle h \rangle$ are subgroups of H of order p with trivial intersection. Since H is abelian,

$$H \cong \langle g \rangle \times \langle h \rangle,$$

and $h_1 g h_1^{-1} = g$ for all $h_1 \in H$.

Now consider the element a of order 2. Since $g \in H$ and H is normal in G, we know $aga \in H$. Then the decomposition of H as $\langle g \rangle \times \langle h \rangle$ gives

$$aga = (g^r, h^s) \quad \text{for some } r, s \in \mathbb{Z}.$$

But a has order 2, therefore

$$(g, e) = g = a(aga)a = (ag^r a, ah^s a).$$

Now $ah^s a = e \Rightarrow h^s = e$ and $ag^r a = g \Rightarrow g^r = g$, using left and right cancellation. Thus $aga = (g, e) = g$. We have shown that g is central in G and so $\langle g \rangle$ is in the centre of G.

Then the solution to Exercise 4.1 gives

$$G \cong \langle g \rangle \times K \cong \mathbb{Z}_p \times D_p\,.$$

(i) Suppose that $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and that G has p^2 elements of order 2. Let a be an element of order 2. Then $G = H \cup aH$ by part (d).

Since $|aH| = p^2$ and since no elements of H have order 2, the product ah has order 2 for all $h \in H$. Thus $ahah = e$ for all $h \in H$, that is, $aha = h^{-1}$. Therefore for $h_1, h_2 \in H$ we have

$$ah_1 ah_2 = h_1^{-1} h_2.$$

We now have enough information to construct a Cayley table for G and so have determined G up to isomorphism.

Index

G/N 33
$\Gamma(\square)$, the symmetry group of a rectangle 13
$\langle g \rangle$ 14
$\cong$, isomorphic to 39

A_n, the alternating groups 11
abelian group 15
action by conjugation 119, 166
action by left multiplication 127
alternating groups 11
associativity 5
automorphism 236

bijection 10
binomial coefficient 208

Cartesian product 88
Cauchy's Theorem 130
Cayley table 12
Cayley's Theorem 128
$\mathrm{Cent}_G(a)$, the centraliser of a in G 169
central element 170
centraliser 169
centre of a group 170
chain of subgroups 187
class equation 168
classification of cyclic groups 102
closure 5
complex number 160
composition series 190
$\mathrm{Conj}_G(a)$, the conjugacy class of a in G 31, 166
conjugate elements 31
conjugate of a by g 165
conjugate subgroups 31
coprime 108
Correspondence Theorem 51
coset 21, 26, 56
cycle form of permutation 10
cyclic group 14

D_4, the symmetry group of a square 13
D_6, the symmetry group of the regular hexagon 13
D_n, the dihedral group of order $2n$ 155
decomposition of $\mathbb{Z}_{mn}$ 112
decomposition theorem for finite cyclic groups 113
Dic_2, the dicyclic group of order 8 159
Dic_n, the dicyclic group of order $4n$ 161
dicyclic group 159–161
dihedral group 155
direct product of groups 89
direct products of cyclic groups 112
direct sum of groups 90
direct symmetry 55
disjoint sets 23

even permutation 10
external direct product of groups 89

finite group 25
First Isomorphism Theorem 49

Galois Theory 191
generalised associativity rule 9
generator 14, 154
$\mathrm{GL}(2, \mathbb{R})$, the general linear group 7
group 5
group action 115
group axioms 5
group presentation 154

highest common factor 107
homomorphism 45
homomorphism property 45

identity element 5
$\mathrm{Im}(\phi)$, the image of a homomorphism 46
index of subgroup 28
indirect symmetry 55
infinite group 25
infinite order of element 43
infinite order of group 25
internal direct product for finite groups 229
internal direct product of groups 94
Internal Direct Product Theorem 95
inverse element 5
inverse of product 6
isomorphism 39

Jordan–Hölder Theorem 190

$\ker \wedge$, the kernel of a group action 181
$\mathrm{Ker}(\phi)$, the kernel of a homomorphism 46
Klein group 37

Lagrange's Theorem 25
least common multiple 108
left cancellation rule 6
left coset 21
length 190

maximal prime power divisor 206
morphism property 45

natural homomorphism 51
normal subgroup 28

$\mathrm{O}(2,\mathbb{R})$, the orthogonal group 13
odd permutation 10
one–one correspondence 10
$\mathrm{Orb}(x)$, the orbit of x 121
Orbit–Stabiliser Theorem 126
order of group 25
order of group element 43
orthogonal group 13

p-group 185
partition 25
partition equation 208
permutation 10
permutation group 10
Prime Power Subgroups Theorem 232
product of cosets 33
product of sets 21
proper subgroup 18

quaternion group 159
quotient group 35
quotients of cyclic groups 104

relations 14, 154
right cancellation rule 6
right coset 26

S_n, the symmetric groups 10
semidirect product 237
simple group 189
$\mathrm{SO}(2,\mathbb{R})$, the special orthogonal group 13
soluble group 191
special orthogonal group 13
$\mathrm{Stab}(x)$, the stabiliser of x 123
standard form 153, 155
subgroup 17
subgroup axioms 17
subgroup conditions 17
subgroup generated by set 162
subgroups of cyclic groups 106
Sylow p-subgroup 206, 215
Sylow Theorems 224
Sylow's First Theorem 206, 215, 217
Sylow's Second Theorem 214, 218
Sylow's Third Theorem 223
symmetric groups 10
symmetry group of X 13
symmetry group of a rectangle 13
symmetry group of a square 13
symmetry group of the regular hexagon 13

transposition 10
trivial subgroup 18
two-line notation 10

underlying set 5
uniqueness of identity 6
uniqueness of inverses 6

well-defined 34, 70
word 154

$Z(G)$, the centre of a group 170
$\mathbb{Z}_n$ 15